Cybersecurity Regulation in the Financial Sector: Reflexive Risk Management in the UK, USA and Nigeria

A thesis submitted for the degree of Doctor of Philosophy in Law

Temitayo Olami Atere

Newcastle Law School

Newcastle University

June 2021

Abstract

The consistent increase in the scale and forms of cyber threats, alongside the growth in use and global uptake of communications technologies, has made risk management a core function of 21st century service providers. This has necessitated the proactive mitigation of cyber threats and the integration of frameworks, policies and regulations that ensure the security of financial transactions. Exploring reflexivity as a mechanism for informing adaptive and resilient cybersecurity risk management practices, this thesis examines structures of coexistence between criminal justice and self-regulatory responses, multiple cycles of reflexive processes of self-examination, participation, communication, and revisions to influence future practices in ever evolving risk and policy landscapes. This thesis evaluates the review, identification, and control dimensions of cybersecurity risk management frameworks, analyses self-regulatory cybersecurity standards and specific cybersecurity legal frameworks applicable to financial institutions in the UK, US, and Nigeria, which can be implemented and/or remodelled to enhance the effectiveness of cybersecurity risk regulation.

It observes that while effective cybersecurity risk regulation across the financial institutions is being hampered by factors such as cherry-picked laws, unclear mandates, and a lack of coordination between public and private stakeholders, strong implementation and enforcement structures may be facilitated by initiatives directed at networked governance and institutional arrangements involving a shared understanding of cyber threats and decision-making processes. This thesis highlights the link between reflexivity and governance for learning in financial institutions, arguing that reflexivity will always not deliver learning, in the absence of good institutional structures of governance. Employing realist and constructivist risk theories and secondary analysis of qualitative data obtained from government and non-government agencies to inform practices and steer regulatory policy decisions, this thesis identifies measures to enhance effective cybersecurity risk regulation in financial institutions and addresses possible challenges to reflexivity in cybersecurity risk regulation.

Acknowledgement

First, I would like to thank God for making this PhD process a success and granting me the strength to conquer every difficulty. This journey would not have been completed without the help and guidance I received throughout.

My deepest gratitude goes to my supervisors Dr Benjamin Farrand, Dr Jonathan Galloway and Dr Abdul Karim Aldohni for their time, wisdom, concern, constructive guidance and support. Their constant prompts on my research writing, their optimism and belief in me were a great source of inspiration. I remain indebted to them. I would also like to thank my thesis examiners, Dr David Reader and Dr Vasileios Karagiannopoulos, for the stimulative discussions and their essential and positive feedback during the viva.

Special thanks go to Dr Francesco De Cecco and Dr Ruth Houghton, for their care, moral support and many productive discussions, as well as to Dr Colin Murray and Professor Daithi Mac Sitigh, my previous supervisors, for their advice and enthusiasm during the early stages of my research. I am also grateful to all staff at the Law School office, in particular Jane and Gemma for their kindness and responsiveness to all my emails, and Gwyneth and Dalia for providing help on several occasions. Likewise, I am grateful to Sue Spencer for the monthly poetry therapy and mental health support. I sincerely appreciate all of the opportunities and financial assistance granted to me by Newcastle Law School.

Importantly, I would like to thank Dr Andrea Miglionico, for having faith in me to pursue the PhD and trusting I would do great. To my siblings, Tosin, Yemi, Deji, Taiwo and Kehinde, I say thank you for your love, solace and consideration. To Emily, Ekor, Ebere, Vickie, Tolu Akinyemi, Tolu Bello and other close friends who were part of the process, I say thank you for your positive energy and reassurance throughout my studies. To my Pastors, the Ladipo's, the Alawode's and the Bamidele's, I am truly grateful for your intercessions, directions and words of knowledge.

My greatest debt is to my biggest cheerleaders, my parents, Olusola and Oluyinka Atere. They, more than anyone, have suffered the financial consequences of my pursuing a PhD. Their patience and relentless support prodded me along, their prayers sustained me in moments of frustration and their encouragement allowed me to complete this thesis.

Contents

Abbreviations

APP	Authorised Push Payment
BoE	Bank of England
BofA	Bank of America
BVN	Bank Verification Number
CAT	Cybersecurity Assessment Tool
CBN	Central Bank of Nigeria
CDA	Cyber Defence Alliance
CEIP	Carnegie Endowment for International Peace
CFPB	Consumer Financial Protection Bureau
CII	Critical Information Infrastructures
CiSP	Cyber Security Information Sharing Partnership
CISA	Cybersecurity Information Sharing Act
CISO/CIO	Chief Information Security Officer
COE	Council of Europe
CPMI	The Committee on Payments and Market Infrastructures
CREST	Council for Registered Ethical Security Testers
CRO	Chief Risk Officer
CSF	Cyber-security Framework
CTCU	Cybersecurity and Technology Control Unit
DDoS	Distributed Denial of Service
DFFKC	Domestic Financial Fraud Kill Chain
DHS	US Department of Homeland Security
DMB	Deposit Money Bank
DoJ	Department of Justice
DPA	Data Protection Act

DPC	Data Protection Commission
EBA	European Banking Authority
ECSB	Economic Crime Strategic Board
EEA	European Economic Area
EFCC	Economic and Financial Crimes Commission
ERM/ERMF	Enterprise Risk Management/Framework
EU	European Union
FACTA	Fair and Accurate Credit Transactions Act
FBI	Federal Bureau of Investigation
FCA	Financial Conduct Authority
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network
FI/FIs	Financial Institution
FMI	Financial Market Infrastructures
FPC	Financial Planning Committee
FSA	Financial Services Authority
FSB	Financial Stability Board
FSMA	Financial Services and Markets Act
FRS	Federal Reserve System
FSARC	Financial Systemic Analysis & Resilience Center
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSOC	Financial Stability Oversight Council
FTC	Federal Trade Commission
GDPR	General Data Processing Regulations
GLBA	Gramm-Leach-Bliley Act
GTBank	Guaranty Trust Bank

ICA	International Compliance Association
IC3	Internet Crime Complaint Center
ICO	Information Commissioner's Office
IEC	International Electrotechnical Commission
IT	Information Technology
IOSCO	International Organization of Securities Commissions
IRM	Independent Risk Management
IRP	Incident Response Plan
ISO	International Organization for Standardization
NAO	National Audit Office
NCA	National Crime Agency
NDIC	Nigerian Deposit Insurance Corporation
NDPR	Nigerian Data Protection Regulations
NeFF	Nigerian electronic Fraud Forum
NFIU	Nigerian Financial Intelligence Unit
NG-CERT	Nigerian Computer Emergency Response Team
NIBSS	Nigerian Inter-Bank Settlement System
NIS/NISD	Network and Information Systems/Directive
NIST	National Institute of Standards and Technology
NITDA	National Information Technology Development Agency
NRC	National Risk Committee
NR	Northern Rock
OCC	Office of the Comptroller of Currency
OCIE	Office of Compliance Inspections and Examinations
OES	Operators of Essential Services
OFR	Office of Financial Research
US-CERT	US Computer Emergency Readiness Team

PCAOB	Public Companies Accounting Oversight Board
PDNPA	Personal Data Notification and Protection Act
PPP	Public-Private Partnerships
PRA	Prudential Regulation Authority
PSD	Payment Services Directive
PSP	Payment Service Provider
PSR	Payment Services Regulations
RAT	IC3 Recovery Asset Team
SEC	Securities and Exchange Commission
SOX	Sarbanes-Oxley Act
SUP	Supervision Manual
SYSC	Senior Management Arrangements, Systems and Controls Sourcebook
UK	United Kingdom
UN	United Nations
URSIT	Uniform Rating System for Information Technology
USA/US	United States of America
USSD	Unstructured Supplementary Service Data

List of Figures

List of Tables

Chapter 1. Introduction

Risks are associated with actions, inactions and omissions which produce potentially uncertain consequences. For instance, outdated IT systems and exploited system vulnerabilities may result in damage to IT systems, network disruptions or loss of sensitive data. Cybersecurity, on the other hand, generally represents the extent to which IT assets, networks and systems are kept secure from cyber threats and attacks. The management of cybersecurity risks is thus the way in which risks to the resilience of IT assets, networks and systems are mitigated, managed and monitored to minimise chances of successful cyberattacks and to increase the likelihood of continuity or rapid recovery in the event of a cyber incident.

While IT has played a major role in enhancing the efficiency, ease and convenience of services provided by financial institutions (FIs), it has also increased the potential for transactions to be affected by cyberattacks. Given that, FIs are continuously developing frameworks with the objective of mitigating risks to the security of their data and infrastructures. Such frameworks are usually composed of policies, guidelines and practices which consider the integration of people, processes, and technology.

Risk management as a long-standing strand of public policy and regulation is thus critical to the attainment of this objective. Particularly, in the financial sector, model risks and systemic risks have remained considerable real concerns for FIs. An examination of model risks which are regarded as an effect of evolving modern risk technologies[1] helps shed some light on the risk landscape in the financial sector. In recent times, studies by Camillo[2] and Gaidosch et al[3] shed light on the management of cybersecurity risks, and call for overarching risk management approaches and resilience-building regulatory supervision of cybersecurity risks to heighten cyber incident response and recovery initiatives and produce more effective regulation.

[1] Mark Carey and René M Stulz, *The Risks of Financial Institutions* (National Bureau of Economic Research 2005) para 2.4.
[2] Mark Camillo, 'Cybersecurity: Risks and management of risks for global banks and financial institutions' (2017) 10 Journal of Risk Management in Financial Institutions 196.
[3] Tamas Gaidosch and others, *Cybersecurity risk supervision* (International Monetary Fund 2019) 1, 7.

Cybersecurity legislative mechanisms must be clear, coherent, appropriate and thoroughly implemented, and must be backed by technological cybersecurity measures adopted by FIs to ensure effective regulation of cybercrimes.[4] Likewise, cybersecurity, though mainly seen as a technology issue is, in reality, also an issue of compliance with relevant regulatory and international standards.[5] Therefore, we proceed with the assumption that if cybersecurity risks must be effectively managed, it is necessary to integrate technological measures with regulatory frameworks, and that this is particularly important to ensure reflexive practices; so that FIs can continuously assess their security measures and learn from its observations, in the face of rapidly changing threats and vulnerabilities.

The journey to effective cybersecurity risk regulation is one of co-existence: how can criminal justice and self-regulatory responses work closely to provide FIs with a seamless regulatory framework for mitigating cybersecurity risks? This is because the complications from choosing one response over the other inevitably involves problems of attributing responsibility and enforcing remedial actions, where self-regulation fails, characterised by problems such as regulatory capture and stifled innovation, to name but a few, where there is excessive government interference.

To address these complications, we must engage mechanisms of 'reflexive modernity' which Ulrich Beck portrays as involving the dialogue, communication, arrangement and nexus of public-private actors in the creation of plans, implementation of frameworks and methods of enforcement.[6] Consequently, it becomes important to explore reflexivity as a means to influence cybersecurity risk management practices in FIs, incorporating repeatable functions and processes of revision whereby decision-making may be adapted to changing risks and regulations, fostering learning and awareness during review and monitoring stages.

[4] Dragos Claudiu Fulea and Marius Ciprian Corbu, *Crime in Cyberspace: Approaches on Legislative Regulation in the Field of Cybercrime* ("Carol I" National Defence University 2014) 323.
[5] KPMG, 'Cybersecurity: It's Not Just about Technology' (2014) <https://assets.kpmg.com/content/dam/kpmg/pdf/2014/05/cyber-security-not-just-technology.pdf> accessed 17 February 2017.
[6] U. Beck and others, *Risk Society: Towards a New Modernity* (SAGE Publications 1992) 199.

1.1 Research Context

Effective cybersecurity risk management is a significant and identifiable objective of the UK,[7] US[8] and Nigerian[9] financial sector, yet its realisation is hindered by a number of factors such as lack of cyber incident reporting requirements, some laxness in the adoption and enforcement of appropriate regulation, conflicting cybersecurity requirements, and certain inadequacies in legislation. This thesis is centred on cybersecurity requirements for FIs in the UK, US and Nigeria, and examines whether existing self-regulatory and criminal justice responses are well-placed to address existing and emerging cyber risks in each jurisdictions. In order to identify best practices or at the very least, settings which facilitate the formation of frameworks and structures for implementing effective and sustainable best practices, it is therefore necessary to consider standards implemented in each of these countries by comparing and contrasting their responses.

Where there are human and technological failings in its IT systems, processes and controls, a bank may be at risk of cyber threats and attacks. A major risk, which is increasingly sophisticated and commonly identified across the case study chapters, is data breach which typically affects the availability, confidentiality and integrity of data. Similarly, unauthorised, remote or card fraud as well as authorised push payment scams have also been identified in these case studies and have significant costs for FIs such as financial losses, loss of trust in e-banking services, disrupted online services, law enforcement costs and security responses.[10]

The extent to which frameworks are implemented varies from country to country with respect to the risks identified in the FIs and regulatory capabilities. In the UK, the framework appears to be a combination of regulatory guidance and requirements on cyber

[7] Financial Conduct Authority, 'Cyber and technology resilience in UK financial services' (14 January 2019) <https://www.fca.org.uk/news/speeches/cyber-and-technology-resilience-uk-financial-services> accessed 10 July 2020.
[8] Congressional Research Service, 'Financial Services and Cybersecurity: The Federal Role' (23 March 2016) <https://crsreports.congress.gov/product/pdf/R/R44429> accessed 10 July 2020.
[9] Nigerian Deposit Insurance Corporation, 'The Impact Of Cybercrime On The Nigerian Economy And Banking System' (August 2020) <https://ndic.gov.ng/wp-content/uploads/2020/08/NDIC-Quarterly-Vol-34-No-12-2019-Article-The-Impact-Of-Cybercrime-On-The-Nigerian-Economy-And-Banking-System.pdf> accessed 10 July 2020.
[10] Ross Anderson and others, 'Measuring the Changing Cost of Cybercrime' (2019) The 18th Annual Workshop on the Economics of Information Security (WEIS) 1, 3.

incident reporting, simulation exercises and third-party risk assessment, risk management processes which emphasise the importance of a Chief Risk Advisor, and regulatory sanctions imposed jointly and individually by the FCA and PRA for cybersecurity breaches. Despite constant efforts by the sector to manage the risks of cyberattacks to its services and develop its systems up to a resilient standard, the current choice of the Payment Services Regulations 2017 and Data Protection Act 2018 as the means of applying cybersecurity legislation to FIs in the UK instead of imposing self-regulatory obligations through the Network and Information Systems Regulations 2018, arguably does very little in facilitating the creation of resilient data, network and information systems.

In the same light, for the US, the increasing costs of cyber incidents in the sector has led to the implementation of measures such as independent risk management functions, involvement of directors in cybersecurity duties, regulatory guidelines on cyber incident reporting, simulation exercises and outsourcing risk assessments, regulatory sanctions by the CFPB and FTC for cybersecurity breaches, and a few prosecutions of cybercriminals owing to collaborations between the financial sector and Justice Department. In addition, there are a number of statutes which specify cybersecurity best practices in FIs, with implications for non-compliance. However, these measures fail to effectively address risks associated with data breaches, which appear to be one of the primary sources of cyberattacks affecting FIs in the US, as observed from the Equifax, First American Financial Corp and Capital One cases.[11] Particularly, the lack of a federal Data Security and Privacy Protection Law leads to inadequacies in data security controls, poor enforcement and conflicting requirements resulting from different state privacy laws.

Designated personnel overseeing cybersecurity policy decisions and a risk-based cybersecurity framework and guidelines on areas such as cyber risk governance, oversight, measurement and incident reporting comprise of measures adopted in the management of cybersecurity risks in Nigeria. In contrast to the UK and US, there is no evidence of any sort of regulatory sanctions imposed against FIs for cybersecurity breaches, despite report from

[11] Carnegie Endowment for International Peace (CEIP), 'Timeline of Cyber Incidents Involving FIs' (2020) <https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide> accessed 10 July 2020.

regulators highlighting cybercrime as the predominant cause of losses in the sector.[12] Moreover, the inadequate and problematic provisions of its Cybercrimes Act 2015 and Data Protection Regulations 2019 place customers in a position of greater risk of cybersecurity breaches and make no specific provision for the reporting of a data breach by the data processor to the controller without undue delay, respectively.

Findings also indicate the lack of transparency and accountability, political influence, lack of division of responsibilities between the regulators and the regulator the Central Bank of Nigeria, duplicity of regulatory authority and inadequate penalty structures as factors which negatively influence the development of a reflexive cybersecurity regulation in Nigeria. Questions of penalty structures prompted considerations of the proportionality assessment on whether the penalties and fines issued are in fact appropriate and justifiable to the conduct being regulated and whether the technical measures implemented by FIs are proportionate to the risks encountered.

Research on the use of reflexivity in labour law,[13] sustainability[14] and public administration[15] reflect the assumption that reflexivity is always good and observe that reflexivity is associated improved regulatory capabilities, change creation and understanding limitations of institutional practices. While this may sometimes be true, it is must also be noted that increased reflexivity does not always equate to increased regulatory efforts and coordination, management and awareness of institutional challenges or new structural transformations. The presence of sanctioning regimes for cybersecurity breaches in the US and UK, and its entire absence in Nigeria which draws its legislative texts explicitly from the US regime, have led us to question the wide suitability of reflexivity.

[12] Nigerian Deposit Insurance Corporation, 'The Impact of Cybercrime on The Nigerian Economy and Banking System' (March 2020) para 6.3 <https://ndic.gov.ng/wp-content/uploads/2020/03/NDIC-Quarterly-Q1-and-Q2-2019-Article-The-Impact-of-Cybercrime-on-The-Nigerian-Economy-and-Banking-System-.pdf> accessed 20 September 2020.
[13] Ralf Rogowski, 'The emergence of reflexive global labour law' (2015) 22 Industrielle Beziehungen/The German Journal of Industrial Relations 72.
[14] Hans Dieleman, 'Sustainability, art and reflexivity' (2008) 108 Sustainability: A new frontier for the arts and cultures 146.
[15] Ann L Cunliffe and Jong S Jun, 'The need for reflexivity in public administration' (2005) 37 Administration & society 225.

Our analysis reveals that in the absence of suitable practices, frameworks and the institutions, reflexivity may not produce required results for regulation, and thus may not always be something to strive towards. They also reveal that a failure in reflexivity does not only come from a failure to learn, but a failure that results from the learning the wrong lessons, which have to be unlearned, and the right lessons learned, in order to adapt to the evolving threat landscape. This finding is consistent with case studies on replication which confirm that sustainable replication can only be aided by learning, experience and strategic investments[16], and when replication fails, it is commonly attributed to key differences and deliberate misrepresentations of the original model.[17] Indeed, key differences to be considered "when making risks decisions are simply not questions on the substance of knowledge" but those which take into account the subject affected, the nature and degree of threat, the characteristics of that threat, the geographical area affected, late and unknown impacts, responses to be initiated, persons' responsible and claims resulting from liabilities.[18] Without these considerations, there can be no real reflexivity within a system.

1.2 Aims and Significance

Viewing cybersecurity risk regulation in the financial services sector under the lens of reflexivity has facilitated the central objective of the thesis to examine the findings of the comparative studies in determining the criminal justice and self-regulatory elements of an effective cybersecurity risk management framework. Given that, this thesis makes a distinct original contribution through the following activities:

i. Proposing the development of a cybersecurity regulatory framework which integrates both criminal justice and self-regulatory responses, which Gaidosch *et al* note must be adaptable to the evolving forms of cyber risks, ensure the enforcement of cybersecurity requirements and provide regulatory authorities with the required scope of supervision[19];

[16] Sidney G Winter and Gabriel Szulanski, 'Replication as strategy' (2001) 12 Organization science 730.
[17] Jeremy Freese and David Peterson, 'Replication in social science' (2017) 43 Annual Review of Sociology 147, 153.
[18] Beck and others, *Risk Society: Towards a New Modernity*, 54.
[19] Gaidosch and others, *Cybersecurity risk supervision*, 12.

ii. Furthering discussions on reflexivity's significant potential, and originally contributes a dimension to the analysis, in Chapter 3, underlining why reflexivity is not always useful and provides targeted answers to the question of how reflexivity can be made useful; and

iii. Identifying the comparative processes that can be used to identify best practices in cybersecurity risk management and the significance of this process in the complete augmentation of the overall regulatory framework, thereby addressing key issues identified in the framework.

While a lot has been written about cybersecurity risks in FIs with limited analysis of the technical and regulatory cybersecurity strategies as a solution for common forms of cyber risks,[20] not enough has been learned about regulatory frameworks for driving effective and proactive management of evolving risks in FIs. No identified literature has discussed the aforementioned issues in a clear, comparative and reflexive fashion, and particularly, no literature has proposed a model for the imposition of individual liability on key decisionmakers responsible for cybersecurity strategy creation and implementation in FIs.

Consequently, this thesis fits well within legal frameworks created for influencing resilient cybersecurity practices as it provides clarity and proposes amendments to the key existing laws, where applicable. The thesis is significant as it will be a major step in analysing the role of regulation to enhance accountability systems in FIs for the management of cybersecurity risks. It will also open new strands of research in the face of evolving cybersecurity risks, which will in turn pave way for advanced policy perspectives for FIs and government bodies involved in the development of cybersecurity risk management frameworks. Therefore, these recognized gaps provide the justification for this research.

1.3 Methodology

As its existing theories and methods are disconnected and insufficient for defining complex situations, quantitative analysis fails to provide interpretations of the impacts of set factors on interactions and subjects under investigation, thus requiring inputs of qualitative analysis to

[20] Examples include phishing, ransomware, hacking and DDoS attacks.

explain or observe varied approaches of the actors in the situations being investigated.[21] This thesis relies on qualitative analysis, and a combination of comparative and socio-legal methods.

The qualitative analysis involved an inquiry into understanding and defining the existing regulatory setting for cybersecurity in FIs in understanding the current regulatory framework governing cybersecurity practices in FIs and examining its effectiveness. Empirical analysis was based on secondary data collected from annual reports and statements of FIs for the year 2019 and reports from government and industry bodies in the UK, Nigeria and USA[22] covering the period of 2016 to 2019, based on the data available. The thesis also examines a wide variety of texts relating to the subject matter, including books, journal articles, online news articles and government publications.

The thesis employs a comparative method for the analysis of the legislation, principles, guidelines and enforcement, governing cybersecurity practices and regulatory structures in the UK, US and Nigeria. The comparative methodology was used to highlight, evaluate and discuss differences, similarities, successes and failures across all three case studies. Do the different regulatory structures facilitate effective cybersecurity risk management? Are there any desirable/beneficial practices? Are regulatory sanctions through the use of penalties and fines enough to discourage reactive behaviours? Are replicated texts effective? Do they require modification to operate similar to the countries being modelled? Is replication necessary at all? To answer these wide-ranging questions, we lend ourselves to the application of comparative methods. Doctrinal and soft law analysis were also used to assess legislation and regulations in the case study countries. Through this, the legal and regulatory standpoints in each jurisdiction were analysed, and regulations, such as the Networks and Information Systems Regulations 2018, were examined by considering approaches to implementation, interpretation of relevant provisions and drawing conclusions from analysis to propose future developments to current frameworks.

[21] Oscar Labra and others (eds), *Thematic analysis in social work: A case study* (Global Social Work-Cutting Edge Issues and Critical Reflections, Books on Demand 2019) 3.

[22] In the US case, data between 2012 to 2015 are included due to the unavailability of up-to-date sector-specific data on remote/payment fraud losses. This is also based on the need to present and analyse the specified data, as done with other case studies.

The socio-legal method on the other hand, is important because it examines the sociological perspectives of risk and places it in the context of the law and explores the influence of regulation in the prevention and management of risks. This method was used in analysing the application of existing cybersecurity requirements under legislation and how they shape the regulation of FIs through an examination of policies and practices adopted by FIs. In particular, it will present the issues arising out of the interaction between legal and social paradigms where the application and enforcement of laws are necessary responses for attributing liability and upholding standards of accountability, where self-regulation fails. A full account of the theoretical framework guiding this project is given in Chapter 3 of this thesis, which is then integrated throughout the subsequent case studies.

The thesis combines the analysis of existing literature, methods and secondary data to simplify, develop and justify the proposed research questions and ultimately ensures that the validity of the research is achieved through the use of triangulation. Besides, triangulation is important as it improves the credibility of data and analysis.[23]

Justifications for Case Study Selection

This case study examines one developing and two developed country cases. Four factors justify the selection of case studies for this research. The first and most significant rationale is the established political ties and diplomatic relations between the UK, US and Nigeria. In particular, Nigeria's adoption of the English common law on account of being a former British colony and the model of its constitution after the US, consisting of executive, legislative and judicial branches of government, provide sufficient justification for comparison. More so, structures of the institutional roles in Nigeria's financial sector and texts in its risk-based cybersecurity framework clearly follows the US regime.

Second, is that it draws upon lessons which can be learned or unlearned from one jurisdiction and applied in some other jurisdictions. In addition, the choice of countries with different legal systems, institutional structures and geographic size facilitates a comprehensive comparative analysis, when examining the self-regulatory responses alongside the criminal justice responses in assessing their adequacy and applicability in each of these systems.

[23] Alain Decrop, 'Triangulation in qualitative tourism research' (1999) 20 Tourism management 157, 161.

Finally, the selection of each country recognizes the possibility that cyberattacks bring about spill over effects that affect other countries due to the interdependence of the international financial system.

1.4 Research Questions

This research aims to answer the following questions:

a. How do self-regulatory responses co-exist with criminal justice responses to ensure effective regulation of cybercrimes and impose liability for cybersecurity failures in the financial services sector?

    i. How do jurisdictions identify the key cyber risks and design appropriate risk management systems, and what commonalities and divergences exist?

    ii. How effective are the self-regulatory responses in each jurisdiction for dealing with existing and emerging cyber risks in their FIs and how do they co-exist with criminal justice responses?

    iii. How effective are criminal justice responses in imposing liability for cyber offences in the financial services sector, where self-regulation has failed?

1.5 Structure of the Thesis

This thesis is divided into seven chapters examining different aspects of risks, regulation and reflexivity, both in theory and practice.

What is cybercrime? Chapter 2 specifically looks at the various cybercrimes considered throughout the thesis, particularly hacking, ransomware and malware, and adopts the use of the term ‘financial cybercrime’ towards highlighting the development of financial crime from traditional white-collar crimes to financial cybercrimes. It briefly outlines the legal consequences of cybercrime, drawing attention to the difficulties around the effective regulation of cybersecurity risks in FIs, and how public-private partnerships may provide an

effective means to enhancing enforcement of cybersecurity regulations, alongside resilient risk management practices and capabilities.

Chapter 3 is a critical literature review of risks, reflexivity and regulation. The chapter starts with a definition of the concept of risk and broad considerations of constructivist and realist theories of risks. It challenges adopting a specific perspective to risks and adapts Beck's pragmatic perspective to risk management incidents. It further discusses the forms and consequences of cybersecurity risks, and as a result considers the relevance of regulation in the implementation of risk management processes. Next, the concept of reflexivity is discussed, invoking a discussion of self-regulation, and its possible challenges and the possible implications of implementing reflexive cybersecurity practices in the financial sector. The chapter ends with an examination of models for the attribution of criminal liability for cybersecurity failings in FIs and questions whether reflexivity is always a good course of action for learning.

What happens where a country explicitly draws lessons from another in terms of the texts, but not in terms of the practice? Chapter 4, Chapter 5 and Chapter 6 critically examine cybersecurity risk management frameworks on a case-by-case basis from a comparative perspective. In particular, they identify components of the frameworks which enhance the cybersecurity risk management capabilities and those which undermine it. Case studies were developed from annual reports, as well as proxy statements and quarterly reports from FIs. Regulatory guidelines and policies were then examined to identify terminologies which explicitly or implicitly inform reflexive cybersecurity practices in FIs. We further examine the 'regulatory co-existence hypothesis' across the UK, US and Nigerian case studies relating to sanctioning regimes, in order to understand (i) the extent to which cybersecurity failures in FIs give rise to intervention for the purpose of law enforcement and (ii) how well this facilitates reflexive learning in relation to the resilience objective. Consequently, a critique of existing cybersecurity legislation in each jurisdiction was carried out to discuss the applicability and enforcement of provisions to the cyber risks identified in each of the cases.

All case studies identify peculiar risks, similarities and differences in the challenges/deficiencies to reflexive cybersecurity regulation and discusses best practices which may or may not produce learning as a result of these case studies. Specifically, Chapter

6 presents instances where there is no learning because there is nothing to learn from, due to governance failures and a lack of well-defined structures and frameworks for assessing the appropriateness of adapted models to the risk environment and for transforming model texts into practice, where applicable.

Chapter 7 summarises key arguments identified in the literature review, and findings drawn from the case studies. The chapter makes recommendations for enhancing cybersecurity risk regulatory frameworks under six headings namely funding, cybersecurity legislation, guidelines and requirements, information sharing, incentivising regulation, penalty and sentencing, annual reports, and voluntary guidelines and policies. It restates the research questions; underlines how this has been answered, discusses implications for future research, theory and policymakers and notes limitations of the research. The chapter concludes that both self-regulatory and criminal justice responses have advantages for risk management, and that effective cybersecurity risk management in the financial sector can be achieved by their co-existence and taking a proactive approach.

1.6 Scope and Limitations

Simon and Goes define limitations as constraints that typically emanate from methodology and study approaches which exceed the researcher's control and potentially alters the research findings.[24] Four major limitations of this research include:

i. the data source i.e., secondary data generated from annual reports and statements, meaning that the research findings are heavily dependent on the accuracy of the secondary data. Difficulties were experienced with gaining access to stakeholders in the financial sector because banks fear reputational and market share risks, thus requiring a consideration of whether secondary data will satisfy the needs of the proposed research.[25]

ii. the various indicators used in the analysis of risk management frameworks in FIs were generated externally and therefore, may not reflect a complete view of each FIs framework indicators.

[24] Marilyn K. Simon and Jim Goes, 'Assumptions, limitations, delimitations, and scope of the study' (2013) Dissertation and Scholarly Research: Recipes for Success 1, 2.
[25] RP Hooda, *Statistics for business and economics* (Vikas Publishing House 2013) 11.

iii. data examined in the US study on sector-specific remote card payments fraud consist of data which is on average 3 years older than those examined in the UK and Nigerian case studies. As such, data does not reflect current threat landscape and comparisons in this respect are limited.

iv. findings from this case study will be limited on the basis of the selectivity of actors who were sampled for discussions[26] and may not be generalised for all FIs as data and analysis involved only two of the largest banks in each jurisdiction examined.

As case studies consist of analysing set units of individual and organisational conducts, they may only suggest possible findings in similar units and may or may not confirm presence of similar conducts in the units but will require deductive quantitative research to validate the generalisability of findings from a single study.[27] Therefore, to validate the generalisability of findings in this case study to a wider group of FIs beyond those studied, quantitative analyses must be carried out to provide a greater degree of accuracy.[28]

The reports and legislation cited in this thesis reflects the information available as at 1 January 2020.

[26] Michael Quinn Patton, 'Enhancing the quality and credibility of qualitative analysis' (1999) 34 Health services research 1189, 1197.
[27] Simon and Goes, 'Assumptions, limitations, delimitations, and scope of the study' 2.
[28] Pamela A Ochieng, 'An analysis of the strengths and limitation of qualitative and quantitative research paradigms' (2009) 13 Problems of Education in the 21st Century 13, 17.

Chapter 2. Financial Cybercrimes in the 21st Century

2.1 Introduction

"Risks are the reflection of human actions and omissions"[1], and cyber risks pose a substantial threat to the stability and resilience of the financial system as the disruption of operations in FIs may lead to large customer, financial and reputational losses, and ultimately harm or cause a breakdown of the global economic system.[2] As a starting point towards the classification of such risks, this chapter provides a preliminary discussion of the various cybercrimes which FIs are at risk of.

With the increase in financial services delivered through the internet, banks are currently at risk of cybercrimes like malware, hacking, phishing and other forms of activity which are constantly being developed, such as ransomware. Securing the privacy and protection of data, networks and systems are now viewed as an issue of major concern for banks. Such concerns expressed in this area relate to "the high level of interconnectivity in the financial industry [which] makes it vulnerable to disruptions", as a DDoS attack[3] on the financial sector supply chain could bring about devastating and spill over effects in the business operations.[4]

There are, at present, extensive categorisations and definitions of the term cybercrime as cyber-enabled, computer-related, internet-related etc.[5] In this chapter, we start with a brief discussion of the scope of cybercrime, its classification under the national legal frameworks of the case study countries and analyse its characteristics and definition. This analysis, as will be seen, provides context for the discussion of prevalent cybercrimes later identified across the thesis. We then briefly discuss the concept of financial crime and provide a taxonomy of emerging cybercrimes in the financial sector, analyse existing literature in the

[1] Beck and others, *Risk Society: Towards a New Modernity*, 183.
[2] Richard Scott Carnell and others, *The law of financial institutions* (Lippincott Williams & Wilkins 2021) 367.
[3] As will be discussed later in this chapter.
[4] EUROPOL, 'Internet Organised Crime Threat Assessment (IOCTA)' (2020) 33 <https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf> accessed 25 May 2021.
[5] As will be discussed later in this chapter. See David S Wall, 'The Internet as a conduit for criminal activity' in A Pattavina (ed), *Information technology and the criminal justice system* (2005/15) 77, 81.

area and adopt the term 'financial cybercrime', on the basis that cybercrimes prevalent in FIs contain some elements of the 'traditional' forms of financial crimes.

Finally, the 'regulatory co-existence hypothesis' emphasised across the case study chapters is introduced here, and arguments are presented with practical considerations for achieving effective public-private coordination in cybersecurity. The chapter concludes with a statement on the major challenges to effective cybercrime regulation in FIs, and an introduction to the concept of risk and reflexive practices employed throughout the later chapters of this thesis.

2.2 What is Cybercrime

Scope

Cybercrime poses a threat to the security of various individuals, institutions, organisations and countries. According to a report by McAfee, the global fiscal cost of cybercrime for the year 2020 is estimated at $945 billion, indicating a 57.5% increase from $600 billion in 2018.[6] Particularly, the report highlights ransomware and financial crime as part of the most-costly categories of cybercrimes. This was observed in an earlier study by Accenture and the Ponemon Institute on the Cost of Cybercrime, in which the Banking sector maintained its position as experiencing the highest average annual cost of cybercrime, with an 11% increase from $16.55 million in 2017 to $18.37 million in 2018.[7] The increasing volume of cyber-attacks have affected the operations of FIs globally and resulted in great financial losses.

While many have agreed on the implications of the internet for cybercriminal conducts, there appears to be disagreement on the risks brought about by such conducts; particularly, assertions around the frequency of cybercrimes, fail to adequately reveal 'what it is that is particularly "cyber" about them'.[8] The risks posed by cybersecurity breaches are

[6] McAfee, 'The Hidden Costs of Cybercrime' (2020) 6 <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf> accessed 17 May 2021.
[7] Accenture and the Ponemon Institute, 'The Cost Of Cybercrime: Ninth Annual Cost Of Cybercrime Study Unlocking The Value Of Improved Cybersecurity Protection' (2019) Fig 3 <https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50> accessed 16 March 2021. Research carried out on security professionals at 355 organisations.
[8] David Wall, *Cybercrime: The transformation of crime in the information age*, vol 4 (Polity 2007) 8.

evolving faster than most legal and technological systems. Farrand considers the genetically uncertain and dynamic nature of technologies and their resulting uncertain risks and questions 'how policy makers [may] effectively govern the security risks of a speculative technology'.[9] He further states the complexities involved in the formal regulation of evolving technologies, where technology moves at a faster pace than regulation and notes that it thus becomes vital to regulate ahead of potential technology threats.[10] Given that, we outline the legal provisions covering the prevalent cybercrimes discussed in the UK, US and Nigerian case studies to provide a useful basis for the subsequent definition of each crime. Although, a detailed critique of the UK, US and Nigerian legal frameworks on cybercrimes is beyond the scope of this thesis.

Characteristics, Definitions and Classifications of Cybercrime

There is no internationally recognised definition for cybercrime. The Budapest Convention (also known as the European Convention on Cybercrime) is the only international instrument addressing cybercrime. The Convention covers a range of substantive offences including "illegal access", "illegal interception", "computer-related fraud" and "data interference".[11] Despite the first attempt by the Convention to classify cybercrimes, no single explicit definition has been provided for cybercrimes. For many years, there has been considerable debate among scholars about the definition and nature of cybercrime. The concept of cybercrime may be understood from an economic, financial, political, scientific and social perspective, in light of its implications.

In the UK, US and Nigeria, certain specific pieces of legislation contain provisions criminalising computer and computer-related crimes. In the UK, the relevant classifications relating to cybercrimes, such as hacking, DDoS attacks and online fraud discussed in our thesis, are contained in sections 1 - 3 of the Computer Misuse Act 1990 and sections 6 - 8 of the Fraud Act 2006. These include: 'unauthorised access to a computer material';[12]

[9] B Farrand, 'Managing security uncertainty with emerging technologies: the example of the governance of neuroprosthetic research' in Antonio Calcara, Raluca Csernatoni and Chantal Lavallée (eds), *Emerging Security Technologies and EU Governance: Actors, Practices and Processes* (1st edn, Routledge 2020) 195.
[10] ibid 197.
[11] Cybercrime Convention CETS 185, Articles 2 - 8.
[12] Computer Misuse Act 1990, Section 1.

'unauthorised access with the intention to carry out or aid the commission of other crimes';[13] 'unauthorised actions which results in or produces a risk of damage to critical infrastructures';[14] and, 'possessing, creating, or supplying materials for use in frauds[15] including *any* programs or data held in electronic form'.[16]

Similar provisions have been provided for in the US, under the Computer Fraud and Abuse Act 1986, Title 18, United States Code, Section 1030 covering 'accessing a computer and obtaining information',[17] 'trespassing in a government computer',[18] 'accessing a computer to defraud and obtain value',[19] 'intentionally damaging by knowing transmission',[20] 'recklessly damaging by intentional access'[21] and 'negligently causing damage and loss by intentional access'.[22]

In the same vein, Nigerian laws classifying these cybercrimes are primarily based on one piece of legislation: the Cybercrimes Act 2015. This covers 'intentional access without authorisation to whole or part of a computer system or network for fraudulent purposes',[23] 'unlawful and intentional commission of an act which causes a direct or indirect serious interference with the computer or system functionality',[24] and 'masquerading as a legitimate organisation in an electronic communication through email messages or links in emails to acquire sensitive information from a victim'.[25] The elements of the offences in the various pieces of legislation could be considered as provisions for cyber-dependent and cyber-enabled crimes, further discussed below.

---

[13] Computer Misuse Act 1990, Section 2.
[14] Computer Misuse Act 1990, Section 3ZA.
[15] Fraud Act 2006, Sections 6 and 7.
[16] Fraud Act 2006, Section 8.
[17] 18 U.S.C. § 1030(a)(2).
[18] 18 U.S.C. § 1030(a)(3).
[19] 18 U.S.C. § 1030(a)(4), when deciding a hacking charge involving fraud, prosecutors are to take into account this provision as a substitute to subsection 1030(a)(2) as hacking offences under (a)(2) may be considered a minor offence in the absence of specific aggravating factors. See US Department of Justice, 'Prosecuting Computer Crimes' 26 <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf> accessed 10 May 2021.
[20] 18 U.S.C. § 1030(a)(5)(A), Sections 1030(a)(5) may be invoked by prosecutors to indict various kinds of acts in US DoJ, 'Prosecuting Computer Crimes' 26.
[21] 18 U.S.C. § 1030(a)(5)(B).
[22] 18 U.S.C. § 1030(a)(5)(C).
[23] Cybercrimes (Prohibition, Prevention, Etc) Act 2015, Section 6 (1).
[24] Cybercrimes (Prohibition, Prevention, Etc) Act 2015, Section 8.
[25] Cybercrimes (Prohibition, Prevention, Etc) Act 2015, Section 32 (1).

Gordon argues that it is a crime that can occur in a wide range of ways and thus defines it as 'any offence aided or carried out by means of a computer, hardware device or networks'.[26] Similarly, Wall defines real cybercrimes as those 'criminal activities initiated or transformed by the internet'.[27] He further classifies cybercrimes into three categories[28] namely: cyber-assisted crimes, cyber-enabled crimes and cyber-dependent crimes. As the name implies, computer-assisted crimes are crimes in which the computer is used to help in the commission of an already existing crime, such that without the computer, the crime could still be committed, but without the advantages provided by technology, such as online fraud. In the same way, cyber-enabled crimes are those which have been enhanced by various new opportunities provided by the internet, some of which have been considered under existing legislation e.g. identity theft, romance scams, pyramid schemes etc. Cyber-dependent crimes, on the other hand, refer to crimes which require the computer, networks or internet for their commission, without which a commission would not occur, such as phishing, hacking and malware, discussed later in the chapter.

Taking a holistic look at each of the classifications above developed by Wall, one soon recognises the differences in the methods of commission[29], catered for under different statutory and criminal justice frameworks.[30] Accordingly, cybercrimes may be grouped under three heads or forms:[31] crimes against machines (computer integrity-related), crimes using machines (computer-related) and crimes in the machines (content-related).[32] Crimes against the machine are criminal activities which compromise the integrity of computer networks and systems access, for example, DDoS, hacking and viruses. Crimes using machines refer to crimes perpetrated by means of networked computers to connect with victims with the aim of

[26] Sarah Gordon and Richard Ford, 'On the definition and classification of cybercrime' (2006) 2 Journal in Computer Virology 13, 14.
[27] David S Wall, 'Policing cybercrimes: Situating the public police in networks of security within cyberspace' (2007) 8 Police Practice and Research 183, 187.
[28] Wall, 'The Internet as a conduit for criminal activity' 81.
[29] For instance, causing harm to a computer, unauthorised access to a computer, unlawful acquisition of personal information online, deception of victims, theft, online violence and obscenity.
[30] Wall, 'Policing cybercrimes: Situating the public police in networks of security within cyberspace' 186.
[31] These are identified as a prototype of the other kinds of cybercrimes in Wall, 'The Internet as a conduit for criminal activity', .
[32] Surian Soosay, ''High risk' cyber-crime is really a mixed bag of threats' *The Conversation* (17 November 2014) <https://theconversation.com/high-risk-cyber-crime-is-really-a-mixed-bag-of-threats-34091> accessed 11 January 2022. The Budapest convention in its Preamble and Arts. 8 and 9 make similar provisions for computer-related offences, content-related offences and offences against the availability, confidentiality and 'integrity' of computer data, computer network and systems.

fraudulently obtaining money, products, or services, for instance, advanced fee frauds, phishing, the compromise of new ecommerce websites etc. Similarly, crimes in the machines are crimes in which computer network systems are used to store the content of computer data such as the exchange and supply of pornographic and hate crime incident contents or contents that aim to debase, harm or instigate hostility.[33]

Wall's use of the word 'machine' may be argued to offer a broader perspective on the classification of cybercrimes on account of the inherent and comprehensive function of the word, such that it could be read in a way which allows us to consider new technologies within the scope of its application. However, the focus of the definitions on the use of a computer has been argued to limit the scope of the classification. Scholars such as Gotterbarn[34] and Beleur et al.[35] have observed that classifying criminal activities carried out using a computer limits the scope of the legal measures developed for addressing such activities as laws are usually developed after the consequences of creating and applying new technologies have been well understood. Particularly, Gotterbarn argues that crime should not be classified according to the equipment with which it was committed as this would create an issue of defining its scope. Given these positions, it is obvious that cybercrime encompasses a wide range of crimes which have been broadly classified as cyber-platform crimes[36], hybrid cybercrimes[37], traditional cybercrimes[38] and true cybercrimes.[39] With this in mind, cybercrime may be defined as a criminal offence wilfully committed, aided or abetted through the deployment on information technology by individuals or organisations acting sui juris. It is also referred to as internet crime.[40] Hence, in the next section, the case for 'financial cybercrimes', and not typically 'financial crimes' is explored.

---

[33] Wall, 'Policing cybercrimes: Situating the public police in networks of security within cyberspace' 186 - 187.
[34] Donald Gotterbarn, *Computer ethics: Responsibility regained* (Honor Society of Phi Kappa Phi 1991) 26.
[35] Jacques J Berleur and Klaus Brunnstein, *Ethics of computing: codes, spaces for discussion and law* (Springer Science & Business Media 1996) 38.
[36] Crimes carried out indirectly using a software (e.g. botnets) as a means of facilitating the commission of other crimes.
[37] Traditional crimes whose nature, mode of commission and impacts have been enhanced through various opportunities provided by the internet e.g. hacking, identity theft etc.
[38] The commission of traditional crimes such as fraud, stalking, money laundering etc, by means of a computer or the internet.
[39] True cybercrimes refer to crimes originating purely from the internet and committed only in cyberspace; Monica Lagazio, Nazneen Sherif and Mike Cushman, 'A multi-level approach to understanding the impact of cyber crime on the financial sector' (2014) 45 Computers & Security 58, 62.
[40] Gordon and Ford, 'On the definition and classification of cybercrime' 14.

2.3 Financial Cybercrimes

The concept of financial crime was traditionally viewed as crimes committed by individuals or institutions against property for the purpose of gaining a personal or financial advantage, for example, forgery, embezzlement, money laundering and others.[41] The International Monetary Fund broadly defines it as '*any* non-violent offence which gives rise to a financial loss.'[42] This definition may therefore be construed to cover a wide range of crimes committed or facilitated using network and IT for obtaining a financial advantage, for example, malware, identity theft, phishing and hacking.

The International Compliance Association (ICA) in its examples of financial crimes emphasizes the significance of emerging financial crimes as it widely interprets it to include electronic crime and information security.[43] In fact, the International Police Organisation offers a more extensive definition of financial crime by stating that it is 'a crime jointly associated with cybercrime which is *often* carried out using the internet and has a negative impact on banking and financial sectors globally.'[44]

Pickett and Pickett define financial crime as a non-violent short-term crime that is generally seen as being less detrimental, but which has an adverse and long term effect on organisations and the economy.[45] To them, types of financial crimes, include the fraudulent use of credit cards by theft or obtaining credit card information from insecure files or forging credit card details onto a new card, diversion of a company's cash for personal purpose and the use of fake websites for advertising attractive items as a way of deceiving customers into making payments for substandard items or no item at all.[46] However, the concept of financial

[41] Agus Sudjianto and others, 'Statistical methods for fighting financial crimes' (2010) 52 Technometrics 5.
[42] International Monetary Fund, 'Financial System Abuse, Financial Crime and Money Laundering - Background Paper' (12 February 2001) <https://www.imf.org/external/np/ml/2001/eng/021201.pdf> accessed 5 March 2020.
[43] International Compliance Association, 'What is Financial Crime?' <https://www.int-comp.org/careers/a-career-in-financial-crime-prevention/what-is-financial-crime/> accessed 2 March 2021.
[44] International Police Organization, 'Financial Crime' <https://www.interpol.int/Crime-areas/Financial-crime/Financial-crime> accessed 18 June 2017.
[45] KH Spencer Pickett and Jennifer M Pickett, *Financial crime investigation and control* (John Wiley & Sons 2002) 2.
[46] ibid.

crime has grown and developed from being classified as a type of fraud to various types of offences which are far more wide-ranging and unlimited in scope.[47]

There are new levels of cybercriminal activities which are more sophisticated than the average traditional financial crime schemes, such that a massive cyber incident that affects the financial sector may threaten its objectives to increase profits at the lowest risk.[48] For instance, data breaches can result in significant harm to the sector's objectives in terms of costs associated with addressing security failings, customer compensation, notification, employing third-party services, aiding law enforcement, and sometimes lawsuits.[49] Hence, in the sub-section below, we consider a taxonomy of approaches to conceptualising financial cybercrimes.

Taxonomy of Financial Cybercrimes

While cybercrime may not prima facie be classified as a financial crime unless its commission manifestly results in economic or financial loss for its victim(s), they are precursors for the other types of emerging financial crimes ("financial cybercrimes"). Financial cybercrimes are now being committed in a highly sophisticated manner using various techniques, for example, phishing, hacking, malware etc., and regulating such evolving crimes presents a significant challenge to FIs. For instance, a hacking attack leading to a data breach may present critical concerns on the 'integrity' of data, that the data being processed, or collected by FIs, has become compromised and inaccurate, and therefore highlights the significance of security breach mitigation measures in the overarching 'information security' framework.[50] In order to understand the nature and impact of financial cybercrimes, we develop a basic framework of classification involving the different aspects of financial cybercrimes, taking into account

[47] Subodh Kesharwani and Shirish Mishra, 'Cybercrime: An Emerging Threat to Banks and NBFCs' (2020) 2 Cybernomics 13, 14.
[48] Lincoln Kaffenberger and Emanuel Kopp, *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment* (Carnegie Endowment for International Peace 2019) 3.
[49] Lance Bonner, 'Cyber risk: How the 2011 Sony data breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches' (2012) 40 Washington University Journal of Law & Policy 257, 263.
[50] Maria Grazia Porcedda, 'Regulation of Data Breaches in the European Union: Private Companies in the Driver's Seat of Cybersecurity?' in Oldrich Bures and Helena Carrapico (eds), *Security Privatization: How Non-security-related Private Businesses Shape Security Governance* (Springer International Publishing 2018) 293.

taxonomies of fraud[51], cybercrime[52], financial crime[53] and financial cybercrime[54] developed in literature.

Figure 2-1 shows a taxonomy of financial cybercrimes which we have developed with specific relevance to this research and uses the method of commission to differentiate each crime for the purpose of classification. The method of commission refers to the criminal activity carried out to facilitate the commission of the offence. Financial cybercrimes are considered to be crimes which occur as a result of the convergence between financial crime and cybercrime. For this reason, the method of commission of most financial cybercrimes overlap each other as they all involve the use of a computer, network or internet.

[51] Naeimeh Laleh and Mohammad Abdollahi Azgomi (eds), *A taxonomy of frauds and fraud detection techniques*, vol 31 (Information Systems, Technology and Management ICISTM 2009 Communications in Computer and Information Science, Springer 2009) 257.
[52] Xingan Li, 'Taxonomy of Cybercrime' (2016) 1 Journal of Legal Studies 1, 4.
[53] Petter Gottschalk, 'Categories of financial crime' (2010) 17 Journal of Financial Crime 441, Figure 1.
[54] Lagazio, Sherif and Cushman, 'A multi-level approach to understanding the impact of cyber crime on the financial sector' Table 1.

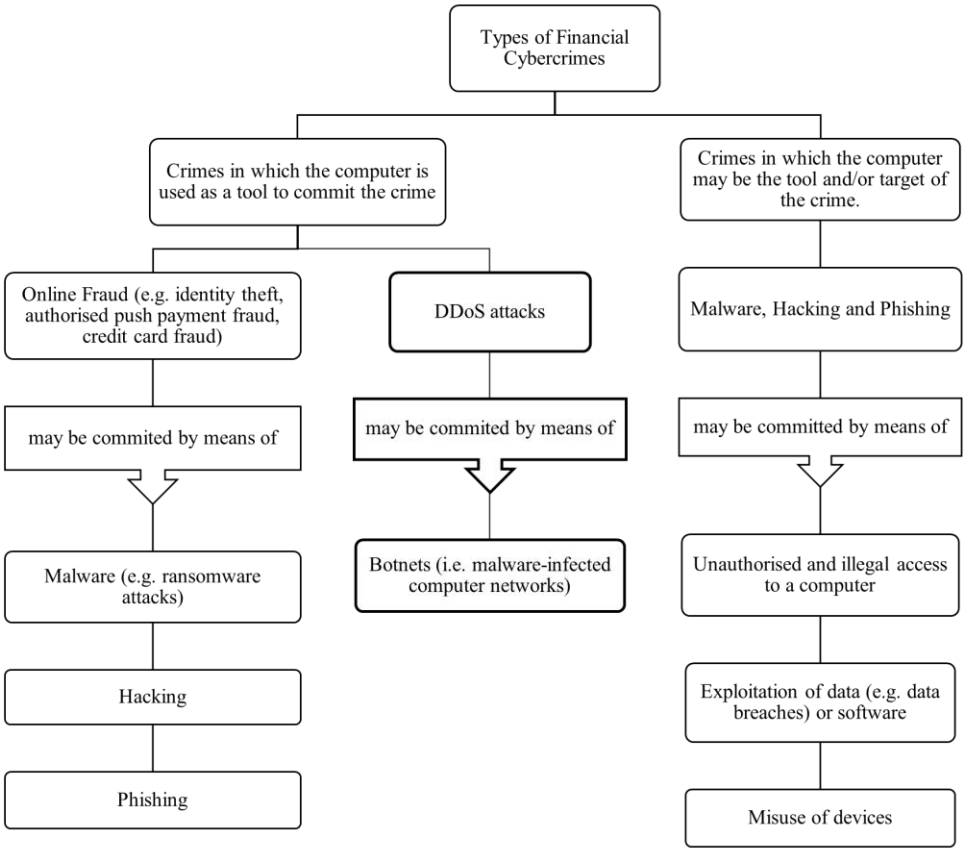

Figure 2-1 Example of a Financial Cybercrime Taxonomy

In ***Figure 2-1*** we illustrate certain similarities and connections between each of these crimes, for instance, hacking may be used in the commission of one or more financial cybercrimes i.e. once a hacker gains unauthorised access into a computer, they are able to steal sensitive information and commit online fraud. Similarly, malware attacks may be used in carrying out both online fraud and DDoS attacks. For example, online fraud could occur where a message pops up on the screen of a computer user requesting for the payment of a ransom to unblock their files or computer as this represents a fraudulent behaviour perpetrated using a computer with the intention of making a financial gain.[55] Having said that, the prevalent cybercrimes in the FIs examined in this thesis are identified below:

[55] Example adopted from - European Union Agency for Network and Information Security (ENISA), 'WannaCry Ransomware: First ever case of cyber cooperation at EU level' *Press Release* (15 May 2017) <https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level> accessed 25 July 2017.

Phishing: This refers to a type of cyberattack which occurs when a perpetrator deceives victims using fraudulent tactics (e-mails containing malicious links, malware advertising etc) into disclosing personal and sensitive data, for example, credit card details, passwords and ATM pins, for gaining unauthorized access, compromising information and causing financial loss. In particular, phishing emails alongside scam messages and data breaches are common precursors to fraudulent card transactions such as unauthorised credit and debit charges, identity theft and card-not-present transactions. Meanwhile, card-not-present transactions create verification challenges for the merchant as it may be complex to tell if it is the cardholder carrying out a transaction.

Online Frauds: The two major types of online fraud considered in this thesis are unauthorised remote banking fraud and Authorised Push Payment (APP) fraud. Unauthorised remote banking fraud is committed *via* the unauthorised access by a criminal into a customer's bank account to carry out an unauthorised transfer of funds from the account through a remote banking platform. The three remote banking platforms include internet, telephone and mobile banking platforms.[56]

APP fraud on the other hand, is committed where a criminal deceives unsuspecting victims into transferring money from their account into a fraudsters account. Different from common types of fraud involving unauthorised access, APP fraud transactions involve authorisation by the customer.[57] This fraud may be committed using email, telephone or text message scams to deceive the victims into paying for goods which they will never receive. For instance, a person may receive an email with the belief that they are being contacted by a legitimate organisation for a particular payment and thus act on it, without knowing they have been defrauded. To conceal the movement of the stolen funds, the criminal transfers the money into several accounts (usually controlled overseas) for it to be withdrawn. As a result, such funds are rarely traceable.

Malware: This may also be referred to as malicious software programmes used to launch unauthorized actions, disruptions and cause harm to a computer system. A malware

[56] UK Finance 'FRAUD THE FACTS 2019: The definitive overview of payment industry fraud' 33 <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf> accessed 2 August 2019.
[57] Anderson and others, 'Measuring the Changing Cost of Cybercrime' 7.

may run on computers, mobile devices or e-banking platforms to gain access to a customer's system and steal personal information or financial data. Types of malware includes virus, trojan, spyware and ransomware.[58]

In the financial services sector, ransomware is especially common and detrimental as cybercriminals are of the notion that FIs have the funds and incentive to pay large ransoms.[59] Ransomware is a form of malware which when present on the victim's computer or system hinders them from accessing their systems or information and demands for a ransom in exchange for restoring the functionality of the system. Most ransomware attacks are launched for the purpose of enrichment, for example, the *WannaCry* ransomware attack which disrupted over 200,000 computer systems in about 150 countries and cost victims about $140,000.[60]

Hacking: This refers to an unlawful access to or intrusion into a computer network or system using another computer to exploit the system or carry out an activity against the actual use of the system. A person who commits hacking is generally referred to as a hacker. Hacking is considered the most common cause of data breaches, which typically brings about risks to the availability, confidentiality and integrity of data discussed in Chapter 3.

DDoS Attacks: This refers to an intentional, temporal or indefinite disruption and interruption to a legitimate user's access to a computer network or system and is generally carried out by botnets, flooding the authorized user's network with large traffic, thus slowing down its function. Cyberattacks using botnets on financial systems have become increasingly popular in recent times. Botnet refers to a collection of internet-connected devices and computers infected with a malware known as bots used by an attacker for control of the affected devices to exfiltrate data, exploit systems, send spam, click fraud etc. Common types of financial botnets include Citadel, Zeus, ICE 1X, Shylock, Bugat, SpyEye and Tinba.[61]

---

[58] Lloyd Bridges, 'The changing face of malware' (2008) 1 Network Security 17, 19.
[59] RSA, 'White Paper: Strategies for Managing Ransomware Risk in Financial Services' (2020) 2 <https://www.rsa.com/content/dam/en/white-paper/strategies-for-managing-ransomware-risk-in-financial-services.pdf> accessed 19 May 2021.
[60] Marshall Billingslea, 'Virtual assets and financial crime now go hand in hand' *Financial Times* (28 October 2018) <https://www.ft.com/content/8e26bba2-d91f-11e8-aa22-36538487e3d0> accessed 19 March 2021.
[61] Aditya K Sood, Sherali Zeadally and Richard J Enbody, 'An empirical study of HTTP-based financial botnets' (2014) 13 IEEE Transactions on Dependable and Secure Computing 236, 246.

The commission of these financial cybercrimes are ever evolving, and both customers and FIs are at risk because of the ease of access and anonymity provided by the internet. FIs and customers are faced with financial loss, depending on whether the customer receives a refund. As a result, strategic steps involving coordinated Public-Private Partnerships (PPPs) and networks must be taken to mitigate these crimes, the risks of which are posed by evolving technologies. These are discussed in more detail below.

2.4 Strategic Management of Cybercrime Risks

A core argument put forward in the succeeding chapters encompasses a 'regulatory co-existence hypothesis' which regard cybercrimes and the resulting risks as security questions whose answers lie in resilience standards that are developed by institutional, cross-sectoral, informational and collaborative elements. Central to this argument is the importance of partnerships in which self-regulatory responses are effectively married with criminal justice responses. Crucial to the success of such partnerships is the dialogue, communication, arrangement and nexus of public-private actors highlighted in Chapter 1, whereby private actors, in this case FIs, act both as regulation adopters and shapers, playing an active role by virtue of their duty as self-regulators to influence cybersecurity policy responses and outcomes.[62]

These partnerships are important as they facilitate effective coordination without excessive oversight from the government, given the shift from imposing commands and monitoring their execution to greater reliance on influencing the framework's setting.[63] In this light, the incorporation of authorities and oversight in legislation will be required to provide regulators with the mandate to create, oversee and enforce compliance with cybersecurity requirements.[64] In other words, laws governing cybercrimes [and regulation specifying

[62] Helena Carrapico and Benjamin Farrand, ''Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers' (2017) 67 Crime, Law and social change 245, 254.
[63] Myriam Dunn-Cavelty and Manuel Suter, 'Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection' (2009) 2 International Journal of Critical Infrastructure Protection 179, 183.
[64] TM Ballou, Joseph A Allen and KK Francis, 'US Energy Sector Cybersecurity: Hands-Off Approach or Effective Partnership?' (2016) 15 Journal of Information Warfare 44, 55.

cybersecurity practices] must be complemented with effective law enforcement at both national and institutional levels in order to mitigate the risks posed by cybercrimes.[65]

As will be argued throughout the thesis, for FIs, a major challenge to effective cybersecurity risk management is the failure to adequately prepare for, communicate, or respond to cyber threats or risks identified, which could result in either mis- or under-reacting to potential threats and consequently, a poorly reactive approach. Moreover, most companies which process large amounts of personal and financial data often detect network and information security failings only after a breach occurs.[66]

When we talk of a poorly reactive approach, we talk of an approach which is largely response-driven, only focused on reacting after the occurrence of a cyberattack and characterised by uninformed, inadequate, and untimely risk decisions. In contrast, a well-organised responsive approach is characterised by its ability to minimise the impacts of cyber threats and attacks and accelerate recovery and business continuity. It is, however, important to note that in the risk management sense, responsive reactive approaches, are to be balanced with fundamental preventative proactive courses of action. Essentially, proactive approaches which are resilience-based, focused on prevention before the breach occurs, mapping out and implementing strategies for the mitigation of future attacks, must be taken into account.

As an illustration, *Equifax*, discussed in more context later in Chapter 5, could have prevented its cybersecurity breaches by applying its set processes for responding to vulnerabilities, developing a detailed IT asset inventory, implementing a proactive patching plan, performing timely follow-up audits, conducting reviews based on results from discussions on its threats and vulnerabilities and, participation of senior management in cybersecurity plans.[67] Upon consideration of proper security measures which could have been implemented against the resulting regulatory, financial and reputational costs of the cyber incident, it becomes clear that such a breach could have been prevented or its impact

[65] Michael L Rustad, 'Private enforcement of cybercrime on the electronic frontier' (2001) 11 Southern California Interdisciplinary Law Journal 63, 99.
[66] Daniel J Marcus, 'The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information' (2018) 68 Duke Law Journal 555, 559.
[67] US Senate, 'How Equifax Neglected Cybersecurity and Suffered A Devastating Data Breach: Staff Report Permanent Subcommittee on Investigations' 21 - 45 <www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf > accessed 15 July 2020 (US Senate Equifax Report).

significantly reduced. The imposition of cybersecurity obligations on FIs, to regulate the failures of self-regulation, becomes therefore a crucial consideration in tackling the misconduct which threatens effective cybersecurity risk management and incentivising/influencing the conduct which strengthens it. This uncertainty in the cybersecurity arena is what has facilitated partnership between various stakeholders, involving both public and private sectors in the planning and implementation of numerous policies aimed at addressing results from risk assessment.[68]

2.4.1 A Case for Public-Private Partnerships in Cybersecurity

Cybersecurity obligations, consisting of technical, management and incident notification guidelines, places the private sector whose operations largely involve data processing, in the 'driver's seat of cybersecurity [vehicle]'.[69] Given that, this vehicle must not be driven blindly nor driven without the wheels of regulation. Indeed, as Porcedda observes, "The fact that the law has the effect of putting private companies in the drivers' seat of cybersecurity does not mean that they will drive down the desired route, without crashing. This ultimately depends on the effectiveness of the incentives and obligations embedded in the law, which may be badly conceived, or wrongly implemented, and which must be discussed as a separate research objective."[70]

Obligations which may be wrongly implemented or badly conceived may be in the form of failing to report cyber incidents or an oversight in the implementation of appropriate network and information systems standards. For instance, if an institution has a poor culture of information sharing and has no [or unclear] 'legal obligation' for information sharing, there is a risk that key information will not be communicated with relevant actors.[71] In the same way, incentives which may be applied include provision of regulatory resources and support e.g. guidelines on incident simulation exercises, cybersecurity training workshops, enhanced information sharing and partnership as well as the use of aggravating and mitigating factors in

[68] Helena Farrand Carrapico and others, 'Disputing security and risk: The convoluted politics of uncertainty', *The Politics of Uncertainty* (Routledge 2020) 153.
[69] Porcedda, 'Regulation of Data Breaches in the European Union: Private Companies in the Driver's Seat of Cybersecurity?' 295.
[70] ibid 276.
[71] Pierre-Luc Pomerleau and David L Lowery, 'Major Themes in the Literature of Cybersecurity and Public–Private Partnerships; A Focus on Financial Institutions' (2020) Countering Cyber Threats to Financial Institutions 87, 94.

determining cybersecurity sanctions. The notion of incentivising institutional behaviour and challenges to the effectiveness of cybersecurity risk regulation are discussed in the following chapter and put into clearer context in the case study chapters.

PPPs are further expressed under the notion of capacity building, which the United Nations refers to as an inclusion of private institutions in broader structures and networks, whereby learning capabilities are improved, resulting in continuous reshaping of these institutions, to enable them to participate actively in strengthening national development frameworks.[72] Mitrou and Karyda identify the implementation of learning capabilities as crucial to the post-incident review stage of cybersecurity risk management in which information sharing with relevant actors, ongoing response assessments, post-response assessments and incident reporting are used to inform risk assessment, build resilience and mitigate future occurrence. [73]

According to Pawlak and Barmpaliou, cybersecurity capacity building may be considered under three interdependent and jointly augmenting levels, namely individual (i.e. skill and knowledge development), organisational (i.e. structural, operational, and network developments) and institutional commonly defined as the 'enabling environment' (i.e. laws, policies and frameworks for the criminalisation of specific conducts).[74] Correlatively, such multi-level frameworks require an implementation of formal and informal processes of obtaining information for learning, developing knowledge and change in practices.[75] Comprehensive cybersecurity capacity building in FIs would therefore involve processes of training, constant threat and risk assessments, established incident response capabilities, cyber risk simulation exercises, collaboration with other stakeholders, implementation of cybersecurity legislation and effective law enforcement.[76] Simply put, PPPs are necessary for

[72] United Nations, 'United Nations System Support for Capacity-Building E/2002/58' (14 May 2002) para 10 <https://digitallibrary.un.org/record/467223/files/E_2002_58-EN.pdf> accessed 10 May 2021.
[73] Maria Karyda and Lilian Mitrou, *Data Breach Notification: Issues and Challenges for Security Management* (2016) 5.
[74] Patryk Pawlak and Panagiota-Nayia Barmpaliou, 'Politics of cybersecurity capacity building: conundrum and opportunity' (2017) 2 Journal of Cyber Policy 123, 124.
[75] Vasileios Karagiannopoulos, *Living with hacktivism: From Conflict to Symbiosis* (Palgrave Studies in Cybercrime and Cybersecurity, 1st edn, Palgrave Macmillan, Cham 2018) 181.
[76] Adapted from Pawlak and Barmpaliou, 'Politics of cybersecurity capacity building: conundrum and opportunity' Table 1.

matching financial sector-specific expertise on cyber threats to public law enforcement and intelligence capabilities.[77]

Where 'collaboration and cooperation' are present, PPPs will facilitate the effective development of cybersecurity and prevention of cybercrimes.[78] However, where they are absent, FIs will be left in a position of no access to vital 'operational and strategic' intelligence information on cyber risk developments and resources for cybersecurity, and participation in collective expert consultations on the identification of best practices in mitigating cybercrimes.[79] Therefore, FIs and other stakeholders must recognise that major challenges must be addressed if the cybersecurity objective is to be achieved.

2.4.2 Challenges to the Effectiveness of PPP in the Regulation of Cybercrime Risks

In a recent study by Pomerleau and Lowery, challenges to effectiveness of PPPs in Canadian FIs were examined, particularly relating to cyber incident information and intelligence sharing. Findings relevant to those of our case studies include challenges of timely communication of cyber incidents and intelligence for prevention, implementation of clear frameworks for information sharing that are cross-sectoral [to prevent a "siloed approach"][80], inadequate legislative frameworks for prevention, conflicting institutional aims and objectives and unclear mandates, functions, and strategies for cybersecurity.[81]

Similar issues were also raised by the European Commission with regards to inadequate cyber threat intelligence sharing structures, conflicting investigative functions, shortage of skilled staff, and poor coordination between actors involved in cybersecurity processes, which had led to the establishment of a European Cybercrime Centre as part of the

[77] Aaron Martin and Valeria San Juan, 'Cyber governance and the financial services sector: The role of public-private partnerships' (2019) Rewired 97, 109.
[78] Jake Rogers, 'Public-Private Partnerships: A Tool for Enhancing Cybersecurity' (2016) 19 <https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/40245/ROGERS-THESIS-2016.pdf?sequence=1&isAllowed=y> accessed 17 May 2021.
[79] Adapted from Benjamin Farrand, "'Alone we can do so little; together we can do so much": the essential role of EU agencies in combatting the sale of counterfeit goods' (2019) 28 European Security 22, 31.
[80] Christian Calliess and Ansgar Baumgarten, 'Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective' (2020) 21 German Law Journal 1149, 1155.
[81] Pierre-Luc Pomerleau and David L Lowery, 'Conclusions and Implications for Practice and Future Studies on Public–Private Partnerships', *Countering Cyber Threats to Financial Institutions* (Springer 2020) 157 - 158.

EU's cybersecurity initiatives.[82] Some of these issues, which are present in our case studies, are also present at a global level and would require multiple partnerships and capabilities to be effectively addressed.

Importantly, there are challenges which affect law enforcement. First, is a lack or inadequacy of penal laws that specifically deal with cybercrime[83] and the problem of relevance, interpretation and capabilities for implementation of cybercrime laws. In this regard, acquiring the capabilities for effective implementation of cybercrime legislation, has been found to present significant issues, especially in developing countries, thereby necessitating total international cooperation.[84] However, there are certain challenges to cooperation at an international level, which may be, for instance, observed from the lack of uniformity among countries with regards to the ratification and implementation of the Budapest Convention.[85] Although, the Convention has been argued to present challenges for effective prosecution by the lack of procedural powers and capabilities required to carry out cybercrime investigations and inadequate criminal legislation for responding to cyberattacks.[86]

Despite the criticisms of the Convention for failing to adapt to rapid technological advancement,[87] Schjolberg applauds it for adopting 'technology-neutral' texts, so that stipulated offences may be relevant to both existing and evolving technologies.[88]. Arimatéia da Cruz echoes its continued relevance, even after almost two decades of being opened[89], yet confirms that the absence of a binding mechanism for the compliance to and enforcement of obligations may negatively affect its objectives.[90] In fact, as will be seen in the succeeding

[82] Communication from The Commission to The Council and The European Parliament, Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre /COM/2012/0140 final/, 3.
[83] Susan W Brenner, 'Cybercrime investigation and prosecution: The role of penal and procedural law' (2001) 8.2 eLaw Journal: Murdoch University Electronic Journal of Law 1, 8.
[84] Jonathan Clough, *The Council of Europe Convention on cybercrime: definingcrime'in a digital world* (Springer 2012) 367.
[85] Susan W Brenner, 'Toward a criminal law for cyberspace: A new model of law enforcement' (2004) 30 Rutgers Computer & Tech LJ 1, 33.
[86] Amalie M Weber, 'The Council of Europe's Convention on Cybercrime' (2003) 18 Berkeley technology law journal 425, 426.
[87] Jianhong Liu, Bill Hebenton and Susyan Jou, *Handbook of Asian criminology* (Springer 2013) 60.
[88] Stein Schjolberg, 'The history of global harmonization on cybercrime legislation–the road to geneva' (2008) 1 Journal of international commercial law and technology 1, 12.
[89] José de Arimatéia da Cruz, 'The Legislative Framework of the European Union (EU) Convention on Cybercrime' (2020) The Palgrave Handbook of International Cybercrime and Cyberdeviance 223, 231.
[90] ibid 234.

chapters, the cybersecurity challenge is not merely one of inadequate legislation for responding to cyberattacks, but one of, in some cases, poor and incoherent enforcement and, other times, inappropriate choice of laws. While international co-operation is important due to the cross border nature of cybercrimes, its discussion is outside the scope of this chapter.

Offences are defined and provided for under legislation to ensure the regulation of criminal conduct and for the protection of a society or nation. It is one thing for the legislators to enact laws which addresses an extensively wide range of cybercrimes, but it is quite another to ensure that these laws are rightly enforced and possess a certain level of flexibility so as to accommodate changes in the field. Although, it is clear that the principle of legality 'nullum crimen et nulla poena sine lege', that is 'no punishment without law', may become threatened by the emergence of new forms of cybercrimes.

The attitudes, methods and targets of cybercriminals are under a constant process of change. And it is this problem, of how detailed or specific or flexible should cybercrime offences be, that seems to be at the core of regulation and enforcement. MacDonald notes that classification of a crime requires specific characterisation and that if the criminal's action is not synonymous with the characterisation, the use of classification for criminalisation becomes ineffective.[91] It is arguable, then, that specifying categories for cybercrimes, if too rigid, may omit considerations for changing risk patterns, regulation and management frameworks which are discussed in later chapters. An updated, adaptive, and constantly reviewed regulatory framework is therefore crucial for facilitating the investigation and prosecution of, and responses to, the advancement of cybercrime.[92]

2.5 Conclusion

In this chapter, we identified various types of cybercrimes and their impacts, and established links between the concepts of cybercrime and financial crime. We also briefly discussed some of the complexities surrounding cybercrime laws and regulation, including challenges to the effectiveness of PPPs and inadequate enforcement. This chapter contributes to our knowledge

[91] John W MacDonald, 'Classification of Crimes' (1932) 18 Cornell Law Quarterly 524, 551.
[92] Marco Gercke, *Europe's legal approaches to cybercrime* (Springer 2009) 410.

and understanding of prevalent cybercrimes in FIs and critically explores their implications for regulation and risk management.

From a reflexive governance perspective, there is a need to develop co-existing structures between public and private actors to address challenges to cybersecurity regulation. This is particularly because the specific structures or groups of structures implemented for cybersecurity have been found to have implications for variations in degree of cybersecurity achieved.[93] While cybercriminals keep developing their techniques, investigating different attack styles, assessing cybersecurity laws and policies, and improving cyber-threat intelligence information sharing are important steps toward ensuring effective cybersecurity risk management.

In the next chapter, we examine these difficulties in more detail and introduce the concept of risk and reflexivity in developing a comprehensive theoretical basis through which we may be able to understand and analyse our case study findings and identify challenges to effective cybersecurity regulation in the financial sector.

[93] Brenden Kuerbis and Farzaneh Badiei, 'Mapping the cybersecurity institutional landscape' (2017) 19 Digital Policy, Regulation and Governance 466, 471.

Chapter 3. The Role of Regulation in Cyber Risk Management

3.1 Introduction

The past financial year has seen a significant rise in the average annual cost of cybercrime to the financial services sector across the globe estimated at $18.37 million.[1] These costs have triggered moves both nationally and internationally toward more security investments and strengthening cyber resilience to tackle cyber threats. In recent times, cyber-attacks and technology failures have become one of the biggest threats to the financial sector capable of causing yet another financial crisis.[2]

Due to the evolving nature of cyber risks, a well-structured *self-regulatory* approach to cybersecurity risks is needed to ensure an adaptive response to the evolving threat landscape, and also enhance the effectiveness of risk resilience frameworks. Financial institutions though largely self-regulated, operate against a backdrop of state regulation, such that in the event of a failure to effectively self-regulate, state authorities may intervene. Interestingly, notwithstanding the acknowledgement of the co-existence of both self-regulatory instruments and state regulation, in many cases, suggested responses to cybersecurity failures in the sector rather tend to be through specialised authorities delegated by the latter. Thus, raising questions on the roles of different stakeholders in regulation, limits to resilience, and different mechanisms in place to monitor and enforce self-regulation.

To promote a better understanding of a well-structured and effective risk regulatory approach, this chapter starts by defining the foundations and theories of risks. This analysis conceptualises risks as a basis for risk regulation further discussed in the chapter. The chapter also discusses the concept of regulation in the financial sector, and the objectives of regulation, thereby highlighting the development of approaches to regulation.

Building on these developments, we examine the theory of reflexivity as a corollary to an effective resilience framework for financial services security. The argument is advanced

[1] Accenture, 'The Cost of Cybercrime - Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection' (2019) <https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50> accessed 27 January 2020.
[2] A. Coburn, E. Leverett and G. Woo, *Solving Cyber Risk: Protecting Your Company and Society* (Wiley 2018) 18.

that, although self-regulation finds its root in reflexive law which suggests that the sector through learning from its failures may correct or prevent future risks; the implementation of procedures, guidelines and other tools of self-regulation may not, on its own, effectively enhance resilience of the sector.

The central point of the issue, it is argued, lies in recognising that achieving the public objective of regulation will, in certain instances, require a coordination between public and private actors. Such a framework is commonplace within the EU in form of a PPP, taking varied institutional shapes and forms.[3] On the whole, understanding the concept of risk and regulation is central to the effectiveness of risk management frameworks as it functions to deal with risks and addresses how the perception of risks may influence relevant actors and policy decisions.

3.2 Defining Risk

Risk assessment and management involves addressing negative situations which present known unknowns risks, unknown knowns risks and unknown unknowns risk, envisaged to occur at some point in time.[4] Hence, to carry out a good risk analysis, the risk assessor must take into account all possible negative outcomes and put in place measures to prevent their occurrence. However, for cyber risks, the risk assessor needs to be aware of the dynamic nature of the risks and the need to carry out a timely review of risks. The objective for financial institutions is then to ensure that they meet relevant security standards and establish controls in place to identify and mitigate cyber risks. Meanwhile, cybersecurity is of major concern to the regulators whose aims are to monitor and transform the conduct of financial institutions to meet required regulatory standards. For instance, a number of jurisdictions have prescribed regulatory requirements requesting banks to create cybersecurity frameworks and

[3] Raphael Bossong and Ben Wagner, 'A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union' in Oldrich Bures and Helena Carrapico (eds), *Security Privatization* (Springer 2018) 220.
[4] Donald Rumsfeld, *Department of Defense News Briefing - Secretary Rumsfeld and Gen. Myers* (US Department of Defense 2002) <https://archive.ph/20180320091111/http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636 > accessed 27 January 2020.

policies that cover areas such as the identification of critical operational assets, cyber-threat reporting and designated responsibilities,[5] which is a central focus of this thesis.

In order to examine the relevant risk-based approaches, it is important to explore the different theories of risk as to explore a single definition of risk would be to limit the understanding and application of risk assessments for decision-making.

3.2.1 Common Theories for Risk Analysis

The different approaches to the concept of risk emanate from different academic disciplines. However, in this research we will examine only social science conceptualisations of risk.[6] One common feature of risk theories is the difference between the real and probable[7] i.e., uncertainties which can be measured and those which cannot be measured[8] tying into the concept of known and unknown risks. These concepts are also used in the objective and subjective context respectively, the former viewing probabilities as real and the latter viewing probabilities as a result of personal opinions.

An understanding of the concept of risk management may be drawn from the works of Stirling,[9] Zimmerman,[10] Bradbury,[11] Giddens,[12] Renn,[13] Clark and Short[14], and Beck[15]. These scholars who contribute to the objective and subjective analysis of risk, examine the two major social theories of risk management, namely realism and constructivism.

---

[5] Juan Carlos Crisanto and Jeremy Prenio, 'Regulatory approaches to enhance banks' cybersecurity frameworks' (2017) Financial Stability Institutions (FSI) Insights on policy implementation 1.
[6] Ortwin Renn, 'Concepts of risk: a classification' (1992) 56.
[7] Ortwin Renn, 'Three decades of risk research: accomplishments and new challenges' (1998) 1 Journal of risk research 49, 51.
[8] Frank Hyneman Knight, *Risk, uncertainty and profit: with an additional introductory essay hitherto unpublished* (London school of economics and political science 1933) 233.
[9] Prof Andrew Stirling, *On Science and Precaution in the Management of Technological Risk: Volume II-case studies*, 1999).
[10] Rae Zimmerman, 'The management of risk', *Risk evaluation and management* (Springer 1986).
[11] Judith A Bradbury, 'The policy implications of differing concepts of risk' (1989) 14 Science, Technology, & Human Values 380.
[12] A. Giddens, *Modernity and Self-identity: Self and Society in the Late Modern Age* (Stanford University Press 1991).
[13] Renn, 'Concepts of risk: a classification' 56.
[14] Lee Clarke and James F Short Jr, 'Social organization and risk: Some current controversies' (1993) 19 Annual Review of Sociology 375.
[15] Beck and others, *Risk Society: Towards a New Modernity*.

The distinction between these two schools of thought lies in their perspective of the nature of risks and its occurrence. The realists perceive that risks and their occurrences are real, observable events.[16] They believe that the real-life calculation of risks amount to a true understanding and judgement of visible threats which can and will bring about consequences predicted by the analysis notwithstanding the opinion of the analysts involved.[17] Realists have been found to conceive risks as being separated from the subjective values advocated by constructivists.[18]

In contrast, constructivists are of the opinion that risk assessment involves a mental construction through societal and cultural standards of uniformity, interrelatedness and internal behaviours of rational deductions. The constructivists believe that risks and their occurrences are social outcomes constructed by societal groups or institutions. Tierney argues that a social constructionist approach does not assert the inexistence of harm,[19] but relies on the assumption that the primary objective is in explaining how stakeholders make use of constructions to arrive at that which presents a danger.[20] Therefore, emphasising that risk assessments cannot merely be adduced from empirical data but also constructed by the individuals who evaluate and experience its consequences.[21] This is echoed in Zimmerman's definition of risk management as the means by which decisions regarding risk are made through combining assessments with the "administrative, legal, political, organizational, and human components of the decision-making process".[22] Stirling notes also, that on the regulation of technological risk issues, a combination of 'best available procedures' and 'best available sciences' in risk assessments, considerations must be given to the array of "perspectives typically brought to bear by different stakeholders".[23]

The realist and constructivist theories pose questions of uncertainty and explanation in terms of whether results of the technical calculation of risks reflects "objective" likelihood of harm or if these calculations represent the culture and practices of a group of professional

[16] Renn, 'Concepts of risk: a classification' 69.
[17] Andreas Klinke and Ortwin Renn, 'A new approach to risk evaluation and management: Risk-based, precaution-based, and discourse-based strategies' (2002) 22 Risk analysis 1071, 1073.
[18] Bradbury, 'The policy implications of differing concepts of risk' 381.
[19] Kathleen Tierney, 'Toward a Critical Sociology of Risk' (1999) 14 Sociological Forum 215, 220.
[20] Clarke and Short Jr, 'Social organization and risk: Some current controversies' 379.
[21] Bradbury, 'The policy implications of differing concepts of risk' 381.
[22] Zimmerman, 'The management of risk' 436.
[23] Stirling, *On Science and Precaution in the Management of Technological Risk: Volume II-case studies*, 76.

risk assessors who admits its claims are valid based on mental constructions solely within the group. In answering this question, Cosgrave notes that one theory must not be chosen over the other as both theories are important for the purpose of understanding the complex and ambivalent nature of risk.[24] The complementary nature of these theories is that which Ulrich Beck observes from a pragmatic viewpoint[25] to be the justification of the world risk society[26]:

> For the one [realists], global dangers must first of all give rise to international institutions and treaties. For the other [constructivists] talk of global environmental dangers already assumes supranational discourse coalitions engaging in successful action.[27]

The classification of risk as a concept which is mentally constructed is formed upon the actual occurrence of the harm, that is, risk outcomes and the perception that human interventions can [significantly reduce] or stop the harm from occurring.[28] This, as some suggest, means that the likelihood of the harm occurring and its seriousness is largely dependent on the relationship between actions or practices and the consequences as the harm may be reduced if the instigating action is controlled and modified or if processes have already been developed to reduce the consequences of such actions.[29] Indeed, an observation of the relationship between risk assessment and constructions, and how risks are categorised reveal actions/processes such as funding arrangements, legal obligations, costs, and resources, and internal organisational politics as having great influence on decision making, and the question of prioritisation answered by conceptualisations of the risk at hand.[30]

According to the World Risk Society theory, risks refer to "a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself."[31] From

[24] James F Cosgrave, *The sociology of risk and gambling reader* (Taylor & Francis 2006) 61.
[25] Beck notes that "the decision whether to take a realist or a constructivist approach . . . [is] a matter of choosing the appropriate means for a desired goal" in B. Adam, U. Beck and J. Van Loon, *The Risk Society and Beyond: Critical Issues for Social Theory* (SAGE Publications 2000) 211.
[26] U. Beck, *World Risk Society* (Wiley 1999) 23.
[27] ibid 26.
[28] Ortwin Renn, *Risk governance: coping with uncertainty in a complex world* (Routledge 2017) 2.
[29] Klinke and Renn, 'A new approach to risk evaluation and management: Risk-based, precaution-based, and discourse-based strategies' 1071.
[30] Julia Black and Robert Baldwin, 'When risk-based regulation aims low: A strategic framework' (2012) 6 Regulation & Governance 131, 146.
[31] Beck and others, *Risk Society: Towards a New Modernity*, 21.

this statement, it is perceived that risk may be equal to processes of risk identification, assessments and management. Some scholars argue against this definition and note that it confuses the idea of risk by equating risks to responses, limiting risk definitions to those presented by modernisation and further taking an inconsistent view on the definition of risk.[32]

While risks cannot solve themselves, the actions taken to prevent or minimise a risk occurrence may in themselves be designated as risks. Heng agrees with Beck as he notes that risk "is not only a descriptive term [denoting a potential danger]; but also, a normative one, implying the need for preventive action".[33] In other words, the risk of using email for multi-factor authentication to prevent the risk of fraud may present the risk of hacking where credentials are vulnerable to interception or spoofing. For instance, when a one-time passcode is sent by email or SMS to prevent fraudulent transactions, there is a risk that user information is not validated and the risk that the expiration time for the code may be so long as to allow the hacker spoof identity information and get a valid unused passcode respectively.[34]

In part, Beck's argument shows an element of foresight as it consists of an attempt to show how the solution to a risk might require the taking of another. Moreover, he immediately contends that "risk as opposed to older dangers, are consequences which relate to the threatening force of modernisation and to its globalisation of doubt."[35] This being the case, Becks definition of risk is admittedly significant as he explores two viewpoints that reflect opposite ends of risk. Nevertheless, to attach the term risk to every action pursued in dealing with hazards/insecurities would be to render risk management impracticable as its full operationality depends on quantifiable uncertainties.

Quantifiable uncertainties refer to risk which in the objective sense views probabilities as real and uncertainties refer to the unquantifiable probability distribution of values[36] which in the subjective context conceives probabilities as a result of personal opinions. While risks refer to instances with measurable outcomes and uncertainties refer to

[32] Scott Campbell and Greg Currie, 'Against Beck: In defence of risk analysis' (2006) 36 Philosophy of the Social Sciences 149, 151.
[33] Yee-Kuang Heng, *War as risk management: strategy and conflict in an age of globalised risks* (Routledge 2006) 71.
[34] G. Najera-Gutierrez and J.A. Ansari, *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux, 3rd Edition* (Packt Publishing 2018) 158.
[35] Beck and others, *Risk Society: Towards a New Modernity*, 21.
[36] Knight, *Risk, uncertainty and profit: with an additional introductory essay hitherto unpublished*, 233.

instances with immeasurable outcomes, the subjectiveness of the latter which allows judgements to be formed about possible consequences solves all problems brought by the distinction.[37] For this reason, financial institutions may resort to taking out cyber insurance policies to assist with minimising and indemnifying them against losses, which Weston and Stigler describe as insurable future outcomes (risks) and uninsurable future outcomes (uncertainties).[38]

After carefully considering these definitions, in this research, we define the term *risk* as the likelihood that an action/inaction or omission or event might bring about vulnerabilities which could potentially cause uncertain events and outcomes to occur such that, if it occurs, has a likely impact (positive or negative) on interests or objectives.[39]

This definition makes use of the term "vulnerabilities", as in the cybersecurity context, to provide an illustration of how an action/inaction or omission or event may cause gaps or weaknesses in security systems, which if exploited by a threat, could bring about negative undesirable outcomes. To illustrate the usefulness of the terms "action", "inaction" and "omission" in the concept of risk, we will consider an artificial situation of three scenarios: Bank A, Bank B and Bank C. Bank A is aware of a loophole in its security systems, it adopts one or more security measures to address this loophole, one of these measures have a vulnerability which could be exploited by a threat or attack, but Bank A does not know about it. Bank B is aware of a loophole in its security systems, it knows the steps it could take to prevent against or manage it but does nothing about it possibly after considering the costs of the security measures or undermining the capability of the vulnerability.[40] Bank C is aware of a loophole in its security systems, it takes steps to protect its systems based on the loophole at hand, without realizing that not all vulnerabilities have been identified. These three scenarios show how a financial institution may be exposed to cybersecurity risks and how the

[37]Geoffrey TF Brooke, 'Uncertainty, Profit and Entrepreneurial Action: Frank Knight's Contribution Reconsidered' (2010) 32 Journal of the History of Economic Thought (Cambridge University Press) 221, 223.
[38] ibid 222.
[39] Definition adapted from Society for Risk Analysis, 'Risk Analysis Foundations' (7 May 2015) 4 <http://www.sra.org/sites/default/files/pdf/FoundationsMay7-2015-sent-x.pdf> accessed 3 December 2017.
[40] Example adapted from Sam Jones and Caroline Binham, 'Cyber security loophole found at bank' *Financial Times* (London, 3 March 2015) <https://www.ft.com/content/d71f8664-c103-11e4-88ca-00144feab7de> accessed 15 December 2017.

management or prevention of these risks could involve an exposure to greater and new forms of risks which are at the core of this research.

3.2.2 What is a Cybersecurity Risk?

Cybersecurity risks are broad, and attaching a single definition to it might raise concerns for risk assessment and management, since its consequences are almost nearly undefined. However, some important variables in the context of cybersecurity risks can be drawn from Beck's definition of modernised risk, in understanding cybersecurity risks as ". . . [risks which are] *systematically intensified* as it becomes *global*"[41] since they follow similar patterns characterised by their "*intractability* . . . the way they spread",[42] thus giving rise to transnational issues.

From the above definition, we identify three features of cyber risks namely: systematic intensity, globality and intractability. Globality looks at the universal consequences of cyber risks i.e., risks which "transcend national borders"[43] due to interconnectivity in cyberspace. Systematic intensity deals with the growing and uncontrollable consequences of cyber risks which affects processes, procedures and systems as a result of their globality. Intractability covers the consequences of cyber risks which are difficult to manage largely due to their incalculableness, but also because its impacts cannot be fully/adequately compensated against. The World Risk Society confirms the global nature of risks and its unequal spread across countries.[44] Using hurricane Katrina as an example, some scholars have argued that in spite of the different levels of development in countries having varying phases of modernity distinguished both locally and internationally, global risks forms an association of countries where the economic and social costs of an incident in one country could spread across to other countries.[45] One such incident was the *WannaCry* ransomware attack which spread across 150 countries and affected various critical infrastructure operators, including finance. Persuasive, if not completely convincing, this idea that countries with different levels of development are

[41] Beck and others, *Risk Society: Towards a New Modernity*, 21.
[42] ibid 40.
[43] Ulrich Beck, 'Critical theory of world risk society: a cosmopolitan vision' (2009) 16 Constellations 3, 6.
[44] Beck, *World Risk Society*, 5.
[45] G. Borne, *A Framework for Sustainable Global Development and the Effective Governance of Risk* (Edwin Mellen Press 2010) 12 - 13.

in one way or another related due to the global nature of security risks experienced in their financial sectors, explain a part of the comparative justifications for this research.

Cybersecurity risks may be classified into risks to information and technology assets (computers, hardware, networks, data communication links etc.) that have the effect of compromising the availability, confidentiality and integrity of data or information systems. The need for entities like, financial institutions to protect against such risks is reinforced in Article 32 of the General Data Protection Regulation (GDPR) which places a legal obligation on the data controller and processor 'to implement appropriate technical and organisational measures comprising of the capacity to ensure continuing confidentiality, integrity, availability and resilience of systems and services processing personal data; and the capacity to reinstate data access and availability promptly in case of a physical or technical incident.'[46]

Availability risks are risks associated with access to information and associated assets,[47] which may occur through IT system failures such that a user/customer is unable to access a service or resource. A common example of this is DDoS attacks. Such risks could arise out of poor data quality, system installations, software upgrades and human errors.[48] These risks are closely connected with Integrity risks in that, an unauthorised alteration and modification of data could result in a denial of service.[49] Addressing such risks would require regular planned system backups, and prevention and recovery from hardware and software errors.[50]

Integrity risks are risks critical to financial services as majority of e-banking services require the use of personal and sensitive data. These are risks associated with data corruption or modification and transactions alterations[51] which may arise where the accuracy

[46] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
[47] Jiri Tupa, Jan Simota and Frantisek Steiner, 'Aspects of risk management implementation for Industry 4.0' (2017) 11 Procedia Manufacturing 1223, 1227.
[48] E.M.C.E. Services, *Information Storage and Management: Storing, Managing, and Protecting Digital Information in Classic, Virtualized, and Cloud Environments* (Wiley 2012) 202.
[49] M.C. Yovits, *Advances in Computers* (Elsevier Science 1994) 2.
[50] C.T. Leondes, *Database and Data Communication Network Systems, Three-Volume Set: Techniques and Applications* (Elsevier Science 2002) 176.
[51] Syed Irfan Nabi and others, 'Data confidentiality and integrity issues and role of information security management standard, policies and practices–An empirical study of telecommunication industry in Pakistan', *Security Technology, Disaster Recovery and Business Continuity* (Springer 2010) 47, 48.

and adequacy of data or its source has been tampered with during IT processes, for example during transmission, processing or storage. Such risks may be addressed by implementing security controls for detecting data alterations. Data integrity techniques include the use of secret passcodes, public key-based digital signature algorithms for data recipient to verify data integrity.[52]

Continuity risks, commonly known as recovery risks, are those which arise from an institution's failure to minimise the disruption to its operations or continue its business processes, after a cyber incident. Such risks may be addressed by proactively implementing adequate and coordinated plans involving staff and frameworks to facilitate the detection, communication and mitigation of cyber incidents,[53] with the plans being assessed, tested and updated regularly.[54]

Confidentiality risks, also known as risks of compromised sensitive data with privacy implications,[55] they cover risks which may arise where unauthorised personnel gain access and control to an institution's computer system and data. Such risks may include identity theft, fraud etc. These risks present a wide range of regulatory concerns such that countries such as the UK and US have enacted legislation to address data privacy breaches.[56] Security of information confidentiality is thus, limiting the access of unauthorised persons to stored, processed/transmitted data as well as subjecting information access control to legal, contractual or business requirements.[57]

Outsourcing risks, as the name implies, are risks to the availability, confidentiality and integrity of customer information which a financial institution knowingly exposes itself

[52] D. Kleidermacher and M. Kleidermacher, *Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development* (Elsevier Science 2012) 305.
[53] T.R. Peltier, *Information Security Policies and Procedures: A Practitioner's Reference, Second Edition* (Taylor & Francis 2004) 157.
[54] P. Trim and Y.I. Lee, *Cyber Security Management: A Governance, Risk and Compliance Framework* (Taylor & Francis 2016) 72.
[55] S. de Capitani di Vimercati, P. Samarati and S. Katsikas, *Security and Privacy in the Age of Uncertainty: IFIP TC11 18th International Conference on Information Security (SEC2003) May 26–28, 2003, Athens, Greece* (Springer US 2013) 279.
[56] In the UK, the principal data privacy legislation is the Data Protection Act 2018, while in the US there is no single principal data privacy Act, but several provisions at federal and state level e.g. The Gramm Leach Bliley Act 1999 and the New York Cybersecurity Regulations (23 NYCRR 500) respectively.
[57] M.C.E. Terrell W. Herzig, *Information Security in Healthcare: Managing Risk* (Healthcare Information and Management Systems Society 2010) 1.

to, where it relies on third-party service providers to carry out certain services for it. Such risks range from unauthorised disclosure of information to financial losses and regulatory consequences.[58] Evidence from case study analysis conducted by Gonzalez et al into financial sector outsourcing indicates that banks outsource significant components of their IT processes for cost-saving, service and process enhancement benefits.[59] The study further highlighted risks such as the absence of outsourcing strategies or policies in banks, lack of regulatory guidelines, supervising the contract and employee transition. To reduce the risks associated with outsourcing, the European Banking Authority (EBA) suggests various criteria which may be weighted and used in the selection of a vendor namely: due diligence checks; risk identification, assessment, management and mitigation processes for potential outsourcing risks; ongoing audit of vendor's performance; compliance with third-party legal and regulatory requirements; and business continuity procedures in the event of a service disruption.[60]

In summary, cyber risks, though less noticeable, are more frequent and difficult to factor and quantify, compared to other financial risks. Indeed, "the way [cybersecurity risks] plays out is too complex to be mapped in advance by mathematics."[61]

Prioritisation, Perception and Management of Risks

Risk management is central to dealing with risks before and after they occur or even at the time of occurrence. Invariably, the decision to avoid or accept certain types of risks form part of the risk management process. In order to make this decision, the implications of risk and its perception must be considered.

One argument Beck offers is that "[r]isks are risks in knowledge, perceptions of risks and risks are not different things, but one and the same."[62] By equating risks to risk

[58] M.R. Overly and M.A. Karlyn, *A Guide to IT Contracting: Checklists, Tools, and Techniques* (CRC Press 2012) 369.
[59] Reyes Gonzalez, Juan Llopis and Jose Gasco, 'Information technology outsourcing in financial services' (2013) 33 The Service Industries Journal 909, 911.
[60] European Banking Authority, 'EBA/GL/2019/02 Final Report on EBA Guidelines on Outsourcing arrangements' (25 February 2019) para 42 <https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1> accessed 11 February 2020.
[61] David Shirreff, *Dealing with financial risk*, vol 41 (UNC Press Books 2004) 38.
[62] Beck and others, *Risk Society: Towards a New Modernity*, 55.

perception, Beck forged what appears to be an anti-risk prioritisation ideology in which multiple risks having different weights may be classed alike, thus blurring the line between perceived and actual risks and resulting in the regulation of too many peripheral risks. Defining risk presents complexities with regards to how risks are understood for the purpose of assessment and management.[63] Bergkamp criticises this idea on the grounds that it provides an unsatisfactory model for risk management decisions, ignoring the degree/level of risks to concentrate on the distribution of risks, thereby resulting in individualised prioritisation and causing generally adverse consequences. He further notes that "it encourages persons, who play a major part in risk society's direct democracy, to concentrate only on the risks to which they experience, regardless of their magnitude".[64] While it is agreed that Beck's definition leads stakeholders to put away significant considerations of the degree of risks[65], it does not, however, follow that it leads stakeholders concentrate only on experienced risks. Instead, it may be argued that it causes them to jumble up both perceived and actual risks such that both are treated equal irrespective of the type, magnitude (low, medium, or high) and criticality of impact. If this happens, the efficiency of the risk management process may be reduced.

Prioritisation in risk management aids the development of a low, medium, or high-risk classification. The underlying basis of risk identification and prioritisation lies in risk assessment i.e. risk estimation and evaluation,[66] also known as risk perception:

> [C]omprising of evaluations of the probability as well as the costs of a negative outcome. Risk perception includes the practice of gathering, selecting and interpreting signals and information about effects of events, activities or technologies in order to form that individual evaluation.[67]

One common practice is seen in how different persons may form different interpretations of risk such that a risk downplayed by one is overestimated by another. Indeed, risk perception

[63] Paul Slovic, 'The risk game' (1998) 59 Reliability engineering & system safety 73, 76.
[64] Lucas Bergkamp, 'The concept of risk society as a model for risk regulation–its hidden and not so hidden ambitions, side effects, and risks' (2017) 20 Journal of Risk Research 1275, 1287.
[65] Relates to both the probability of the event's occurrence and also to the estimated outcome in terms of the nature, intensity and duration of the adverse effects in Vincent T Covello and others, *Uncertainty in risk assessment, risk management, and decision making*, vol 4 (Springer Science & Business Media 2013) 242.
[66] William H Bassett, *Clay's handbook of environmental health* (Spon 1999) 202.
[67] Janina Hofer (2016) 'Report on risk perception: Deliverable D32.1 for Driver Project' <https://driver-project.eu/wp-content/uploads/2017/11/Report-on-risk-perception.pdf> accessed 5 December 2019.

maintains the concept that societal input may shape risks into what is 'tolerable, acceptable or unacceptable'.[68] That is, there are risks which an institution will accept based on its profits and low cost of management, there are also risks which an institution may be willing to tolerate where the profits are high and the risks of losses are low if risks are properly managed and, there are risks which are unacceptable where the losses perceived are high or the costs involved in risk management outweighs the expected benefits. Beck argues against defining acceptable levels of risks, noting that:

> Acceptable values may indeed prevent the very worst from happening, but they are at the same time 'blank checks' to poison nature and mankind *a bit*. How big this 'bit' can be is what is at stake here.[69]

This appears to put forward a question: At what point do the acceptable levels of risks become unacceptable? To answer this, it is the point where cyber risks go beyond a permissible state. Given this, it is reasonably expected that risk levels specified in a cybersecurity framework are to include measures which minimise risks to an acceptable level. Thus, to define acceptable levels of cyber risks, there must be policies, guidelines and frameworks in place which explicitly outline this, and this will vary across financial institutions because what might seem an acceptable level to one might be unacceptable to another. As Beck puts it, "if one permits toxicity at all, then one needs an acceptable level decree."[70]

In sum, risks perceptions consist of real and hypothetical risks, some of which may be tackled by proactive risk management processes. Renn notes that risk management may mean that, sometimes management actions may be taken prior to risk assessments on the basis of factors which either form part of or are uninfluenced by the assessment outcomes.[71] Proactive risk management is thus important when one considers cybersecurity risks, as the different perceptions of risk would influence the probability of an institution to implement detection, monitoring and response controls for mitigating the likelihood and impacts of

[68] Basel Committee on Banking Supervision, 'Compliance and Compliance Function in Banks' (April 2015) <http://www.bis.org/publ/bcbs113.pdf> accessed 10 September 2017.
[69] Beck and others, *Risk Society: Towards a New Modernity*, 64.
[70] ibid 65.
[71] Renn, *Risk governance: coping with uncertainty in a complex world*, 7.

security incidents. In other words, the justification for a proactive approach or acting with little understanding of potential risks.

Risk management is concerned with the prevention of future security incidents by providing an opportunity to develop timely solutions and management approaches.[72] Beck sums up the risk management process as ". . . the modernisation process [transformed] into a *learning process*, in which the revisability of decisions makes possible the revocation of side effects discovered later."[73] In essence, risk management assumes the application of knowledge in adapting already made decisions to *avoid* or *reverse* negative consequences in the future. Furthermore, the dynamic nature of cyber risk and its outcomes makes it almost impossible to measure its impact accurately; however, a meaningful measurement of cyber risks would involve a timely review of risk assessment to keep track of evolving risks. Situations such as these, also help to highlight the importance of regulation in overseeing the conduct and misconduct of financial institutions. This draws together the realist and constructivist approaches articulating how through the constructions of risks, norms emerge towards the regulation of conduct to mitigate risks identified in assessments. This integration is shown in the move of financial regulators worldwide towards developing frameworks in respect of cybersecurity risks encountered by financial institutions. For example, as far back as 2014, UK financial authorities developed the CBEST, an intelligence-driven framework used in assessing and testing a firm's IT or cyber resilience for the purpose of increasing the understanding and awareness of firms on the forms of cyberattacks which affect the stability of UK financial markets as well as the degree of vulnerability of the market to those attacks.[74]

Ultimately, the importance of ensuring the cyber resilience of financial institutions cannot be underestimated and is reinforced by their status as critical information infrastructures (CIIs) [75] as they depend greatly on information technology and thus a single

[72] Tony Ryan, *Managing crisis and risk in mental health nursing* (Nelson Thornes 1999) 3.
[73] Beck and others, *Risk Society: Towards a New Modernity*, 178.
[74] Bank of England, 'CBEST Intelligence-Led Testing: An Introduction to Cyber Threat Modelling' *Version 2.0* (2016) 19 <http://www.bankofengland.co.uk/financialstability/fsc/Documents/anintroductiontocbest.pdf> accessed 15 September 2017.
[75] These may refer to ''Information and communication systems and services which are critical infrastructures for themselves or that are necessary for the proper functioning of critical Infrastructures (e.g., computers/software, internet and telecommunications) "in Council Directive 2008/114/EC of 8 December 2008 on The Identification and Designation of European Critical Infrastructures and The Assessment of The Need to Improve Their Protection.

breach to their network and information systems can result in a disruption, destruction and failure in operations. In this regard, certain legislation like the Network and Information Systems Directive (NISD) imposes specific obligations on the operators of essential services to assess, manage and mitigate risks to their network and information systems[76] as well as notify relevant authorities of cyber incidents with a significant impact.[77] In order to discuss financial risk regulation frameworks in detail, we need to first define what regulation is, why we regulate and how regulation operates.

3.3 Understanding Regulation

Definition of Regulation

Generally, regulation is considered as the creation of rules by the government, which it implements, monitors, and enforces either by itself or through a mandate given to governmental institutions or other non-governmental institutions. Such institutions may include central banks, financial services authorities, or other agencies.

Baldwin et al, suggest three definitions of regulation:[78] First, as the "promulgation of mandatory set of rules backed by procedures for supervision and enforcement to ensure compliance"; second, as "all procedures carried out by institutions of the state to direct the economy"; and third, as "all instruments of social control or influence, including incidental and non-state procedures". Other scholars have also considered the interventionist approach to regulation which involves a direct intervention in the economy by the government.[79]

The first two definitions suggested by Baldwin et al are the ones commonly used by the government, since they are focused on the state and the use of legal measures. Black criticises this as a narrow view of regulation, noting that it fails to consider other systems of

[76] Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, para 44.
[77] Network and Information Systems Directive, Article 14.
[78] Robert Baldwin, Colin Scott and Christopher Hood, *A reader on regulation* (Oxford University Press 1998) 3 - 4 and R. Baldwin, M. Cave and M. Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (OUP Oxford 2012) 2 cited in Christel Koop and Martin Lodge, 'What is regulation? An interdisciplinary concept analysis' (2017) 11 Regulation & Governance 95, 95.
[79] Martín Molinuevo and Sebastin Sez, *Regulatory assessment toolkit: A practical methodology for assessing regulation on trade and investment in services* (World Bank Publications 2014) 60.

monitoring and enforcement.[80] Black echoes the sentiments of Selznick[81] and defines regulation as "the sustained and focused attempt to alter the behaviour of others according to defined standards[82] or purposes with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of setting standards, information gathering and behaviour modification".[83]

By this, Black's reference to sustained, implies an element of intention i.e. the exercise is conscious of the purpose which it seeks to achieve, may be quite broad depending on the context, and may require the use of systems which establish guidelines and gathers information in taking the necessary steps for influencing the behaviours of people. This sustained and focused attempt, as Majone notes, will at some point require the establishment of designated agencies responsible for "fact-finding, rulemaking, and enforcement".[84]

Smith sheds light on the controversial consequences of Black's definition, the most relevant being the consideration of pluralist forms of regulation; the conceptualisation of regulation and how this relates to the intrinsic nature of regulation which focuses on modifying or adjusting behaviour.[85] This conclusion sets out a crucial inference of how regulation considers decentred approaches as opposed to other common definitions and how it encourages plurality in definitions of regulation. Given that, interactions may arise between various forms of public and private regulation, whereby diverse principles, ideas and norms become interdependent to produce a collaborated regulation, which may in one way or the other influence behaviour. This approach thus recognises regulatory shortcomings which may arise from focusing on a single regulatory mechanism and suggests that regulation constituted by different techniques, may produce a more generalisable, yet effective result.

[80] Julia Black, 'Decentring Regulation: Understanding the role of regulation and self-regulation in a'post-regulatory'world' (2001) 54 Current legal problems 103, 129.
[81] Philip Selznick, 'Focusing organizational research on regulation' (1985) 1 Regulatory policy and the social sciences 363 cited in Koop and Lodge, 'What is regulation? An interdisciplinary concept analysis' 96.
[82] Standards may consist of resource contributions, processes, productions or outcomes and can be directed at a number of aims including best practice/effectiveness, equality and quality (Oliver James, 'Regulation inside government: Public interest justifications and regulatory failures' (2000) 78 Public Administration 327, 328).
[83] Julia Black, 'Critical reflections on regulation' (2002) 27 Australian Journal of Legal Philosophy 1, 25.
[84] Giandomenico Majone, 'The rise of the regulatory state in Europe' (1994) 17 West European Politics 77, 81.
[85] Dimity Kingsford Smith, 'What Is Regulation-A Reply to Julia Black' (2002) 27 Australian Journal of Legal Philosophy 37, 43.

Centred and Decentred Approaches to Regulation

The 'command and control' refers to an old but, dominant paradigm of regulation in which, a government sets out rules or standards of behaviours to be followed and enforces sanctions in the event of any breach.[86] Sinclair describes it as a form of regulation where the government employs the use of laws (directly) or delegated institutions (indirectly) to *command* the adherence of industries to certain defined standards, and exercises the use of negative sanctions to *control* its behaviour.[87] The regime finds it basis in the deterrence theory which proposes the use of express and carefully drawn laws, and the threat of penalties as punishment for deviant behaviour to prevent offending.[88] Traditionally, this model has been relied upon by government regulators in the creation and implementation of policies as it is believed that restraining or limiting certain activities would help influence behaviours. However, some scholars have disputed its efficacy on the basis that this model consumes too many resources in maintaining strategies for monitoring and sanctioning of inappropriate behaviour[89] and legally, that these sanctions have little or no effect on bad behaviour.[90]

Many scholars, however, now advocate for a decentred approach to regulation. Such advocates tend to veer from assumptions that the government is the only one with power to command and control effectively,[91] and look towards the existence and intricacies of the interaction and interrelationship between social actors and between the government and social actors.[92] This argument appears logical when one considers that the society consists of different individuals, including those who manage various firms or businesses and recognising that identifying government as the only actors capable of regulation is like assuming that only a part can form a whole instead of a two-way concept in reality.

[86] Christopher Hodges, *Law and Corporate Behaviour: Integrating Theories of Regulation, Enforcement, Compliance and Ethics* (Bloomsbury Publishing 2015) 166.
[87] Darren Sinclair, 'Self-regulation versus command and control? Beyond false dichotomies' (1997) 19 Law & Policy 529, 534.
[88] Jenny Job, Andrew Stout and Rachael Smith, 'Culture Change in Three Taxation Administrations: From Command-and-Control to Responsive Regulation' (2007) 29 Law & Policy 84, 87.
[89] Donald C Langevoort, 'Monitoring: The behavorial economics of corporate compliance with law' (2002) Columbia Business Law Review 71, 118.
[90] Hodges, *Law and Corporate Behaviour: Integrating Theories of Regulation, Enforcement, Compliance and Ethics*, 167.
[91] Black, 'Critical reflections on regulation' 3.
[92] ibid 5.

Black criticised the view of the state as the only source of legitimate regulation, noting that such approach is unilateral as the legal rules backed by threat of sanctions are basic and unsuitable, with inadequate knowledge for determining the causes of problems, thereby making it impossible to identify non-compliance and develop appropriate measures.[93] Truly, when rules are too prescriptive, there tend to be many conflicting approaches to application or even many cases of non-compliance where rules are too complex or non-reflective of the current position or expectations of society. Galligan observes that:

> Regulatory law requires compliance with standards that often (but not always) are contrary to the interests of those required to comply with them, and that often (but again not always) lack deep or social moral foundations. The consequence is that those to whom the standards are addressed have no clear or strong reason to comply (beyond the fact that it is a legal standard), with the further consequence that enforcement or the threat of enforcement by coercion becomes a necessary feature of regulatory regimes.[94]

This implies that the 'command and control' regulation is not sufficient and cannot be justified beyond the fact that it is a legal instrument, since regulatory laws are viewed as compulsory standards which people must comply with whether they are attuned to their social beliefs or not. Whether they like it or not is equally immaterial, it is simply law, which those who propagated or enacted believe to be for the good and orderliness of the society.

Given the nature of law, it seems only logical to consider sanctions as one of the main instruments for enforcing regulations and ensuring compliance, but a more pragmatic approach would be indirect, one which focuses on the objectives and standards to be met. Moreover, criminal sanctions are hardly ever imposed[95] as most regulatory offences carry civil or administrative sanctions, except for very serious offences e.g., insider dealing and market abuse which may attract custodial sentences and maximum financial penalties, as they

[93] ibid 3.
[94] Denis Galligan, *Law in modern society* (OUP Oxford 2006) para 8.5.
[95] Hodges, *Law and Corporate Behaviour: Integrating Theories of Regulation, Enforcement, Compliance and Ethics*, ch 8, pt II. Criminal sanctions are not often used in the enforcement of regulations as they have been criticised as indulgent and having no deterrent effect on law breaking behaviours.

raise economic and social policy concerns. Typically, the implementation of regulation takes the form of an informal process, a guidance, rather than a command.[96] Such informal practices have been found to be pervasive throughout the regulatory enforcement process.[97] By contrast, Rakoff[98] and Arbel-Ganz[99] believe that the implementation of regulation is a product of formal and informal processes where the former exercises oversight over the latter. These processes take the form of an arrangement, an understanding and a negotiation between regulators and those being regulated. With this type of regulation, there is no direct interference with the behaviour of the regulated persons or firms either through ordering them or specifying consequences. Instead, their behaviours are influenced through establishing guidance with coercive foundations as a backdrop in recognition that legal standards can be enforced at last resort.[100] At the same time, this implies that regulations cannot exist without an element of coercion even though the 'command and control' strategy is criticised as being inappropriate through its use of threats of sanctions. In other words, 'the idea of the shadow of the law' is what makes the guidance more respected and desirable.

The development of arguments in this thesis is based on the understanding of indirect influence of the law embedded in the concept of self-regulation, where 'the actions of regulated agents are guided by developed standards of behaviour and a duty to ensure compliance of its members, with consequences stipulated for misconducts'.[101] Self-regulation is an important aspect of the decentring argument "…as a feature of autopoietic closure, [and] is central to the decentring analysis".[102] The concept of autopoiesis which has a biological origin and characterised by its dynamicity is used to refer to a system which maintains or transforms its structure.

[96] Galligan, *Law in modern society*, para 8.5.
[97] Bronwen Morgan and Karen Yeung, *An introduction to law and regulation: Text and materials* (Cambridge University Press 2007) 151.
[98] Todd D Rakoff, 'The Choice Between Formal and Informal Modes of Administrative Regulation' (2000) Administrative Law Review 159, 170.
[99] Ori Arbel-Ganz, 'Formal and Informal Regulatory Networks: Deliberative Policy Formation in Israel' 18.
[100] Galligan, *Law in modern society*, para 8.5.
[101] Jari Råman, *Regulating Secure Software Development: analysing the potential regulatory solutions for the lack of security in software*, vol 102 (Lapland University Press 2006) 179 - 180.
[102] Black, 'Decentring Regulation: Understanding the role of regulation and self-regulation in a'post-regulatory'world' 128.

In the context of regulation, particularly self-regulation, autopoiesis refers to a system with a dynamic structure which changes based on the systems own norms and values[103], characterised by self-regulation, self-reproduction, and self-reference.[104] It has been observed as a principal diagnosis of regulatory failure, and posited normatively as the key to regulatory success".[105] This is, however not true, as autopoiesis has led to the regulatory failures highlighted in some historical events. For instance, the 2007-2008 financial crisis caused largely by self-regulatory approaches in financial markets, with very minimal regulatory oversight[106], where regulatory standards were found to be watered down due to errors in estimation of risks.[107] Institutions have been regarded as autopoietic systems for their roles in addressing cybersecurity incidents involving a new autopoietic system of small processes, developing its own systems and self-reproducing in its own practices as incidents are addressed by designated incident management procedures and teams.[108]

What happens where incident recovery processes fail due to information asymmetries in decision-making or habitually poor implementation of security practices as a result of weak monitoring? Besides, regulatory mechanisms used in decentred approaches have been seen as problematic as it arguably undermines regulatory standards.[109] Will autopoietic systems' continue to focus only on internal learning processes? No, they must operate against a backdrop of law to establish systems of accountability i.e., self-reproducing guided by external learning processes to effectively regulate against such failures. Having the potential to be present in more than one environment, autopoietic systems steer the activities in each environment towards self-replication through a symbiotic model[110] i.e. they are shaped in symbiosis deploying theoretical dialogues as self-reproducing processes of

[103] Black, 'Critical reflections on regulation' 17.
[104] Bob Jessop, 'State theory, regulation, and autopoiesis: debates and controversies' (2001) 25 Capital & Class 83, 86.
[105] Black, 'Decentring Regulation: Understanding the role of regulation and self-regulation in a'post-regulatory'world' 128.
[106] Eric Helleiner and Stefano Pagliari, 'The end of self-regulation? Hedge funds and derivatives in global financial governance' (2009) *Global Finance in Crisis: The Politics of International Regulatory Change* 134.
[107] Jeffrey Friedman and Richard Posner, *What caused the financial crisis* (University of Pennsylvania Press 2011) 288.
[108] Pasi Hyytiäinen, 'Sharing cyber threat intelligence in cyber exercise: Does controlled sharing of threat intelligence improve situation awareness?', JAMK University of Applied Sciences 2018) 17.
[109] Matthew Kalkman, 'Re-Assessing Regulation in Light of the Financial Crisis' (2010) Inter Alia 96, 100.
[110] J. Achterbergh and D. Vriens, *Organizations: Social Systems Conducting Experiments* (Springer Berlin Heidelberg 2010) 127.

transformation.[111] The symbiosis model involves a step by step, informed, and multidimensional process primarily carried out to propel change 'through the setting of smaller changes in motion rather than immediate and radical paradigm shifts that more appropriately describes the way multi-actor regulation could work' in a well-developed and mutually integrated regulatory system consisting of key actors, functions, practices, customs and organisational components[112] - a fundamentally ideal blend of both the criminal justice and self-regulatory systems.

Murray illuminates the benefits of symbiotic regulation and the risks of direct government intervention: the benefits resulting from effectively connecting existing networks between the actors and the risks from a direct interference into the stable regulatory environment with severely subverted implications.[113] Symbiosis in respect of autopoietic regulation is the steering wheel that allows subsystems change and develop through communication involving three crucial elements: 'what is being communicated,' 'how, to whom and when it is being communicated,' and 'the meaning perceived by the recipient of the communication', all of which steer the self-replicating autopoietic course through repeated "communications".[114]

It therefore follows that the characterisations of autopoietic systems by unities and interactions between producing components,[115] may suggest the collaboration and interdependence of different regulatory structures (governmental and non-governmental) in the realisation of regulatory objectives. Decentring regulation is concerned with a restructuring of the role of the government and of the nature of interactions that exist within the society (and is prompted by the quest for more effective frameworks of regulation and, by the realisation that the occurrence of particular types of social activities should be made subject to certain values and appropriate objectives).[116] It may involve the use of private rules (e.g. rules of an organisation, firm or industry) and establish practices or institutions which

---

[111] P. Schumacher, *The Autopoiesis of Architecture, Volume I: A New Framework for Architecture* (Autopoiesis of architecture, Wiley 2011) 82.
[112] Karagiannopoulos, *Living with hacktivism: From Conflict to Symbiosis*, 180.
[113] Andrew Murray, 'Symbiotic Regulation' (2008) 26 The John Marshall Journal of Information Technology & Privacy Law 207, 224 - 225.
[114] ibid 226.
[115] Felix Geyer and Johannes van der Zouwen, *Sociocybernetic Paradoxes: observation, control and evolution of self-steering systems* (Sage 1986) 174.
[116] Black, 'Critical reflections on regulation' 28.

have no basis at all in long-established principles of law.[117] Although, government regulation is often *via* the use of laws and sanctions, and if one acknowledges a regulatory style that is not 'state-centric', the implication of this is dissociating regulation from the activities of the government.[118]

Clearly, the decentred approach has a significant impact on the relationship between law and regulation as it places the law within the wider sphere of regulation, as opposed to the traditional approach where regulations are seen as being derived from the law.[119] By so doing, the law maintains its role as one of the forms of social control 'to channel individuals into orderly behaviour'.[120] As Sinclair notes, theories on separating government authority and self-regulation are at best spurious and allowing both actors to regulate together, may effectively develop policy options.[121]

Considerations for Implementing Regulatory Mechanisms

According to Black, regulators take into account a number of factors in determining how to prioritise their regulatory mechanisms. Firstly, operational drivers resulting from limits to the legal, informational, management and resourcing frameworks and positions of regulators.[122] Regulators will often perform their duties on the basis of the legislative mandate set out by parliament which clearly defines their objectives.[123] One common objective found in the policy document of most financial regulators is the prevention of systemic risk or risks which may threaten the stability of the financial system. Such risks may arise from cyber-attacks to CIIs which have a potentially negative impact on financial stability.

Also, in risk identification, when a regulatory body is faced with making trade-offs, it will often times depend on the interpretation of its mandate and sometimes this might lead to a series of repetition.[124] A legal mandate without adequate enforcement powers limits the

[117] Smith, 'What Is Regulation-A Reply to Julia Black' 40.
[118] Black, 'Decentring Regulation: Understanding the role of regulation and self-regulation in a'post-regulatory'world' 129.
[119] Kalkman, 'Re-Assessing Regulation in Light of the Financial Crisis' 99.
[120] Robert F Meier, 'Perspectives on the concept of social control' (1982) 8 Annual Review of Sociology 35, 42.
[121] Sinclair, 'Self-regulation versus command and control? Beyond false dichotomies' 541.
[122] Robert Baldwin and Julia Black, 'Driving Priorities in Risk-based Regulation: What's the Problem?' (2016) 43 Journal of Law and Society 565, 573.
[123] Transport Research Centre and International Transport Forum, *ITF Round Tables Port Competition and Hinterland Connections*, vol 143 (Organization for Economic 2009) 42.
[124] Baldwin and Black, 'Driving Priorities in Risk-based Regulation: What's the Problem?' 574.

capacity of regulators in carrying out thorough risk profiling. This is because all regulators might not have the necessary tools to identify risks and in instances where these risks have been identified, they might not have the enforcement powers.[125] In the case of cyber risks, there might be challenges associated with the failure of taking a proactive approach or not employing appropriate responses to evolving risks that it is faced with.

In addition, the funding arrangement of a regulator can also affect its choice of regulation. As regulators in certain industries are financed by licence payments received from the regulated entities, and fees paid are usually dependent on the risk level[126], regulators are driven to structure risk identification accordingly. In addition, different units within a regulatory agency can also construct risk identification differently, and this may lead to conflicting approaches.[127] For instance, in financial institutions, the perspective of the chief information security officer, will vary differently from those of cashiers, managers and shareholders as they all play different roles in the bank, with respect to cyber risk management. Another issue closely tied with this is the diverse interpretations by different actors as to what amounts to a 'material' cyber incident and if it should be communicated. As such, the diverse interpretation/construction of risk and the models for information sharing are generally believed to assist in the understanding of risks. However, it has been observed that pragmatic regulators will often choose to 'collect only information that is collectable'.[128]

As a final point, the multi-level governance framework structure which requires interactions at national, regional and international levels contain many obligations for financial institutions and expectations to uphold accountability and legitimacy towards various legitimacy communities.[129]. Most financial regulators in the UK operate under EU regulatory regimes and are also connected to other global regulatory structures such as the Financial Action Task Force, International Monetary Fund, International Organisation of Securities Commissions (IOSCO) and G20.[130] The standards formulated by these regimes

[125] Aditya Narain, Ms Inci Ötker and Ceyla Pazarbasioglu, *Building a more resilient financial sector: Reforms in the wake of the global crisis* (International Monetary Fund 2012) 86.
[126] Baldwin and Black, 'Driving Priorities in Risk-based Regulation: What's the Problem?' 575.
[127] ibid 576.
[128] ibid 577.
[129] ibid 578.
[130] Renate Mayntz, *Negotiated reform: The multilevel governance of financial regulation*, vol 85 (Campus Verlag 2015) 10.

have also shaped the decisions of regulators with regards to the construction, assessment and profiling of cybersecurity risk. For instance, the UK's implementation of the EU NIS Directive[131] as the NIS Regulations 2018.

3.4 A Move towards Reflexivity in Financial Sector Cybersecurity

Typically, 'reflexivity' may refer to the state in which modernisation 'becomes its own theme'[132] i.e. exercising constant self-reflection aimed at continuous self-development. It is also regarded as the adaptability of major facets of social activities, and significant relationships with the world, to constant modification, given new information or knowledge.[133] Hence, it supposes a cycle, a state of replication and reoccurrence in the foundations of an organisation's design, for the purpose of assessing the adequacy of existing solutions:

> A reflexive orientation does not ask whether there are social problems to which the law must be responsive. Instead, it seeks to identify [and explore] opportunity structures that allow legal regulation to cope with social problems without, at the same time, irreversibly destroying patterns of social life.[134]

The philosophy underpinning autopoietic law, (decentred regulation and self-regulation) stems out of this orientation, theorised as the self-reproducing nature of social subsystems.[135]

Consistent with Beck, Kuhlmann et al make use of the phrase *learning process* to explain tentative governance as an on-going, never ending and flexible exercise to manage interdependencies and uncertainties.[136] This form of governance has been found to function in

[131] Directive 2016/1148 of the European Parliament.
[132] Beck and others, *Risk Society: Towards a New Modernity*, 19.
[133] Giddens, *Modernity and Self-identity: Self and Society in the Late Modern Age*, 20.
[134] Gunther Teubner, 'Substantive and reflexive elements in modern law' (1983) Law and society review 239, 274.
[135] Peer Zumbansen, 'Law after the welfare state: Formalism, functionalism, and the ironic turn of reflexive law' (2008) 56 The American Journal of Comparative Law 769, 791.
[136] Stefan Kuhlmann, Peter Stegmaier and Kornelia Konrad, 'The tentative governance of emerging science and technology—A conceptual introduction' (2019) 48 Research policy 1091, 1093.

the ‘shadow of hierarchy’[137] to which some maintain that ‘politics (the state) [acting behind the scenes] would demonstrate a more *preserving effect*’ where it lays down the entire (juridical) requirements and monitors the general applicability of regulations over the ‘fictitious power constructions (self-regulatory bodies)’ which overshadow it.[138] Tentative governance in light of reflexivity embraces a progressive rationale in pursuit of solutions to uncertainties and changes, and acknowledges the likelihood of unplanned consequences of governance while reflecting on the starting point.[139] Suggesting a similarity between decentred regulation and reflexivity, Beck notes that*:*

> [*O*]*rganisational power migrates from the domain of politics to that of sub-politics* [and that] everyone else – even the most responsible and best-informed people in politics and science – more or less lives off the crumbs of information that fall from the planning table of technological sub-politics.[140]

He suggests a useful interpretation of politics and sub-politics as they relate to the regulation of self-regulation: in politics, there are *indirect* sources of authority which may be exercised during lengthy ‘implementation periods’ in sub-politics to provide further opportunities to monitor, manage and reduce risks.[141] Zumbansen suggests that these *indirect* sources of authority may include “. . . legal intervention [which are] to take place or to be withheld in accord with, and in response to, the "needs" of a functional group.”[142] While this may be true, the argument assumes that the efficacy of self-regulation may only be fully reached with the intervention of the law. This is explained through a range of hypotheses: the threat of intervention may prompt private actors to self-regulate effectively; may influence non-governmental actors seeking to escape intervention to continuously strive towards self-

[137] Adrienne Héritier and Dirk Lehmkuhl, 'The shadow of hierarchy and new modes of governance' (2008) 28 Journal of public policy 1.
[138] Beck and others, *Risk Society: Towards a New Modernity*, 235.
[139] Kuhlmann, Stegmaier and Konrad, 'The tentative governance of emerging science and technology—A conceptual introduction' 1094.
[140] Beck and others, *Risk Society: Towards a New Modernity*, 223.
[141] ibid 209.
[142] Zumbansen, 'Law after the welfare state: Formalism, functionalism, and the ironic turn of reflexive law' 796.

regulation; may stop the projection of costs of self-regulation to the public; and may enhance the effectiveness of sectoral governance, where sanctions/requirements are imposed.[143]

Self-regulation, the "object of all the various 'solutions' [diagnoses the] regulatory failure that lies at the heart of the decentring analysis."[144] Black echoes these views stating that this new conception of regulation is founded upon the normative characteristic of the *indirect* intervention in the self-regulation of social actors, in that it harnesses self-regulation to achieve public policy objectives through "adjusting, balancing, structuring, facilitating, enabling, and negotiating".[145]

A fundamental aspect of decentred regulation is a significant shift from 'regulatory law' which defines 'substantive standards' to 'reflexive law' which defines 'procedures', with the latter focused on enhancing the reflexivity of structures and their adaptability to their social conditions, reflected in the harmonisation or collaboration of viewpoints between various public-private actors or structures.[146] In this regard, reflexive law is seen as an instrument of indirect intervention to facilitate and empower, where the subsystems are believed to be well developed to promote social structures.[147] Black recognises this relationship shift as the "de-apexing of the state, but notes that hierarchy will always lurk behind heterarchy, and negotiations will always be in its shadow."[148]

Some scholars consider self-regulation to be reflected in the government to governance approach i.e. a permanent change from hierarchical political regulatory structure to a heterarchical one of differing and incompatible regulatory frameworks, where the legal outcomes previously entirely drawn in the building of political governance, turns highly uncertain.[149] Also regarded as a contract between government actors and actors of sectoral governance (private/non-governmental actors), it allows for the modification of the contract to new developments, for settling issues in the implementation of the inadequate contract and for

[143] Héritier and Lehmkuhl, 'The shadow of hierarchy and new modes of governance' 3.
[144] Black, 'Decentring Regulation: Understanding the role of regulation and self-regulation in a'post-regulatory'world' 125.
[145] ibid 126.
[146] ibid 126 - 127.
[147] Zumbansen, 'Law after the welfare state: Formalism, functionalism, and the ironic turn of reflexive law' 796.
[148] Black, 'Decentring Regulation: Understanding the role of regulation and self-regulation in a'post-regulatory'world' 145.
[149] Zumbansen, 'Law after the welfare state: Formalism, functionalism, and the ironic turn of reflexive law' 774.

guaranteeing compliance with its terms.[150] Risk management is very important in such context, where it necessitates co-operation and partnership between various actors.[151]

The participation of non-governmental actors in regulation is argued to help determine relevant issues and facilitate the creation of suitable policy proposals, as the greater say they have in policy decision-making, the greater the likelihood that they will be receptive to the policy results to be implemented, even if all their interests may not have been completely catered for.[152] In particular, the collaboration of various social actors in regulating cyber threats may trigger or will trigger two types of responses, one from the top in form of international treaties and institutions and the other from the bottom, in form of new transnational actors working past parliamentary political structure and challenging conventional interest groups/political associations.[153] This extensive global chain of regulation exists solely as a result of the global nature of the threat at hand. While there is significant evidence of the latter response, there appears to be very little evidence for the former as there is only one international treaty on cybercrime[154] which was reached almost two decades ago. As of December 5, 2019, the treaty has only been ratified by 64 countries, majority of which are Eastern European countries. Countries such as Nigeria and Russia which have the highest population in their respective continents and are associated with top cybercriminal gangs and/or organising numerous cyber-related crimes are yet to sign and ratify the treaty. Nevertheless, there are regional movements in the EU relating to cybersecurity regulation such as the EU Cybersecurity Act, GDPR and NIS Directive. The huge growth of cybercrime in recent years need to be accompanied by effective regimes consisting of new international treaties and institutions supported by all nation states, particularly the great powers or an update and universal implementation of existing alternatives.

Overall, self-regulation appears to solve the dilemma and helplessness of the law's exposure to cyberspace, which really, can be summed up in a single sentence. That is, self-regulation eases the tension created by law's exposure to innovation and its risk to facilitate

[150] Héritier and Lehmkuhl, 'The shadow of hierarchy and new modes of governance' 4.
[151] Renn, *Risk governance: coping with uncertainty in a complex world*, 7.
[152] Tanja A Börzel, 'Governance with/out Government' (2010) False promises or flawed premises 19.
[153] Beck, *World Risk Society*, 37.
[154] Budapest Convention on Cybercrime.

an adequate level of security, provide safeguards, and allocate responsibility for possible risks/harm and equally eliminate roadblocks to innovation.[155] In this light, regulators need to allow banks to innovate freely, together with the recognition that cyber risk regulation is important in the face of evolving technologies and highly sophisticated attacks.[156]

The effects of regulation on innovation have been the subject of considerable debate among scholars.[157] Innovation is central to any economy as it paves way for the development and application of new ideas which provides advantages and solutions to the society. Particularly, innovation in the financial services industry is important as it provides opportunities for exploring new technologies. As such, regulation becomes especially crucial for ensuring that these innovations are not exploited to commit cybercrimes. With this in mind, the prospects of innovation may be influenced either negatively or positively by regulation. Indeed, there is the possibility that regulation may hinder some technologies developed for providing cyber threat solutions. For instance, innovations like biometric encryption and cryptography, beyond the scope of this thesis, may raise regulatory concerns over privacy rights and data protection, relating to a customer's personal control over how their data is used and an institution's responsibility to protect data collected.[158] There are also issues as to whether sufficient regulatory frameworks are present at national and international level for collecting, storing and sharing data.[159]

Generally speaking, most countries have already adopted privacy or data protection laws, even though some of these laws have no sufficient provisions for new forms of data and may potentially affect innovation. Meanwhile, other countries like the US, in our case study, who are yet to adapt a universal data privacy and protection law, arguably deprives its citizens

[155] Maria Weimer and Luisa Marin, 'The role of law in managing the tension between risk and innovation: Introduction to the special issue on regulating new and emerging technologies' (2016) 7 European journal of risk regulation 469.
[156] Consultancy UK, 'Regulation should not crush innovation in financial services sector' (25 October 2017) <https://www.consultancy.uk/news/14262/regulation-should-not-crush-innovation-in-financial-services-sector> accessed 22 January 2018.
[157] See Robert C Merton, 'Financial innovation and the management and regulation of financial institutions' (1995) 19 Journal of Banking & Finance 461 and Knut Blind, Sören S Petersen and Cesare AF Riillo, 'The impact of standards and regulation on innovation in uncertain markets' (2017) 46 Research Policy 249.
[158] Bank of England, 'The Promise of FinTech – Something New Under the Sun?' (25 January 2017) <https://www.bis.org/review/r170126b.pdf> accessed 5 March 2018.
[159] ibid.

and critical sectors like banking and insurance of frameworks which facilitate a more uniform approach to the implementation of data protection policies, structures and procedures.

Regulation is delegated to specialised institutions or agents by political principals and may be attempted out for various reasons:[160] First, in view of the significant operation costs, it helps to guarantee adequate expertise, particularly the lack of expertise of political actors (e.g., in member states and the EU) in policy decision-making. Second, it helps to promote consistency and predictability of policymaking. Then, it helps to address the delays of previous financial market regulations.

As Majone observes, the delegation of regulation from the state-sector presents an alternative for seemingly more effective, policy methods without eliminating regulation.[161] For instance, the substitution of regulatory standards (e.g., laws) by incentives (e.g., charges) or as in this case, replacing stringent legal requirements with network and information security standards and guidelines to promote best practices. In other words, the state-sector arrangement, does not seek to force compliant behaviour, but rather to influence it. This supports the decentred argument for a lesser amount of restrictive or direct regulation in pursuit of alternative means to realise pertinent regulatory aims.[162] Despite this, the distinction between direct regulatory instruments and incentive-based methods have been contested on the basis that the latter imitates some characteristics of the former. For instance, to ensure the implementation of best practices and to prevent firms from escaping liability, complex system of rules are in place which can sometimes be backed by checks and enforcement.[163]

3.5 Possible Challenges to Self-Regulation

A common challenge to self-regulation is the overlapping mandates or operations of relevant actors. Where there are multiple actors in government and governance, findings have shown

[160] Héritier and Lehmkuhl, 'The shadow of hierarchy and new modes of governance' 9.
[161] Giandomenico Majone, 'From the positive to the regulatory state: Causes and consequences of changes in the mode of governance' (1997) 17 Journal of public policy 139, 143.
[162] Majone, 'The rise of the regulatory state in Europe' 80.
[163] Baldwin, Cave and Lodge, *Understanding Regulation: Theory, Strategy, and Practice*, 112.

less efficacy, where competition among principals lessens their regulatory capacity over agents.[164]

Another possible challenge may be lack of transparency in communications within the subsystem. One such argument highlighted by Beck was the untrustworthiness of risk experts as they are being employed by the governments and organisations responsible for polluting the environment. In the context of our research, this argument could be translated to mean that evidence showing the measure of cyber risks in financial institutions may be unreliable where those employed to carry out risk assessments have some form of association or interests in or the institutions themselves having some form of relationship with the government. Beck argues that:

> The production of risks and their misunderstanding . . . is directed at the advantages for productivity. Hence it is also stricken with a systematically conditioned blindness to risk. The very people who predict, develop, test and explore possibilities of economic utility with all the tricks of the trade, always fight shy of risks.[165]

By this, Beck suggests that the miscalculation of generated risks by risk experts, is attached to some productivity-related benefit, which causes them to constantly avoid confronting risks. From this, he makes an entirely broad and strong assertion that risk experts have a "permanent compulsion"[166] to misrepresent and refute truly existing risks and are thus, seemingly untrustworthy.[167] The main question, therefore, is whether case study examples from the financial sector in developed and developing economies will enable us make such general claims i.e. demonstrating how these claims extend in practice where cyber risks have been intentionally underestimated for political, reputational, financial benefits etc. or whether these claims can be contested in practice due to other regulatory difficulties.

[164] Héritier and Lehmkuhl, 'The shadow of hierarchy and new modes of governance' 14.
[165] Beck and others, *Risk Society: Towards a New Modernity*, 60.
[166] Ulrich Beck, *Ecological Politics in the Age of Risk Polity Press* (Cambridge 1995) 86.
[167] Campbell and Currie, 'Against Beck: In defence of risk analysis' 154.

3.6 Possible Implications of Reflexivity in the Financial Sector

Applying the theory of reflexivity to financial sector cybersecurity requires implementation of an effective regulatory framework, one which enables relevant supervisory or regulatory authorities to constantly adapt and enhance the sector's resilience to existing and potential cyberattacks. When choosing which guidelines, principles, codes of conducts or requirements to implement, regulators are to have regard for those which offer flexibility according to the changing risk landscape.

Of great importance, is incident reporting which helps inform the decisions of social actors regarding changes in risk management processes that are needed to tackle current and potential cyber threats. It is especially important for financial sector principals and agents alike to review such reports and develop countermeasures or apply corrective measures accordingly. Such reports encourage reflexivity through developing response plans and creating awareness of security risks towards sector risk-management. While a holistic outlook on global cyber incident reporting in the financial sector appear relatively inconsistent and low, the financial sector may be well served in advance, by regular assessments of an institution's cybersecurity frameworks using simulation exercises, recovery testing etc. These constant exercises are a useful way to assess the efficacy of existing risk management processes against desired objectives. Indeed, a reflexive legal framework seeks to formulate decision-making processes within institutions in such a way that the public policy objectives are realised.[168]

3.7 Proactive and Reactive Regulation in the Financial Services Sector

The maxim, "An ounce of prevention is worth a pound of cure" in the context of cybersecurity basically means that the implementation of proactive measures to prevent future cyber incidents may be more desirable than introducing reactive measures to address a successful cyber incident. While a proactive approach may not always prevent the materialisation of cyber incidents, it may at the very least minimise its effect.

[168] Black, 'Decentring Regulation: Understanding the role of regulation and self-regulation in a'post-regulatory'world' 127.

Reactive and proactive regulation are two strategic approaches to regulation which are complementary in nature and also underpinned by the principle of reflexivity. Reactive regulation deals with newly made decisions and actions implemented in response to a cyber incident. Proactive regulation, on the other hand, deals with the decisions made and actions taken before a cyber incident is at hand. While one seeks to address cyber incidents at hand, the other seeks to prevent cyber incidents from arising in the first place. Therefore, reactive regulation requires an alteration of regulation already in place and proactive regulation intends to enhance the efficacy of future regulation.

A major argument in favour of reactive form of regulation is that due to the ever evolving uncertain nature of cyber risks, high uncertainty regarding any weaknesses may not be cost-effective for proactive implementation as an institution is ill informed on which asset to safeguard and thus, may decide to take no precautions until vulnerabilities are exposed.[169] Some scholars suggest that cybersecurity is the "state of normality" arising out of a combination of proactive and reactive measures such as guidelines, frameworks, ethics and strategies for training and awareness, security, risk management, and implementation of technical measures to defend IT systems and incident management.[170]

Others note the absence of a clear line between both approaches, recognising that how each approach is defined is susceptible to change over time due to the evolving nature of technology e.g. the proactive exercise of changing a password quickly becomes reactive where the user is exposed to a breach possibly from using the same password across multiple interfaces and thus, needing to act as a result of this failure.[171] Generally, security strategies involve a range of both approaches in which security vulnerabilities are (predicted) and technical solutions integrated into IT processes for prevention and also responding to existing threats with the standard technologies to effectively counter security risks.[172]

Indeed, it may be argued that a more effective risk management model for the financial services sector would require a combination of both approaches while giving more

[169] Juhee Kwon and M Eric Johnson, *An Organizational Learning Perspective on Proactive vs. Reactive investment in Information Security* (Citeseer 2011) 6.
[170] Cezar Peta, 'Cyber-Security-Current Topic of National Security (I)' (2013) 2 Studii de Securitate Publica 66.
[171] M.P. Gallaher, A.N. Link and B. Rowe, *Cyber Security: Economic Strategies and Public Policy Alternatives* (Edward Elgar Publishing, Incorporated 2008) 72.
[172] ibid 98.

strength to proactive approaches, to better achieve its objectives of cybersecurity more realistically and appropriately. Besides, it would seem unlikely that a completely reactive or proactive risk regulation exists. The forms of action which each approach may involve are indicated in the table below:

Reactive regulation	• assessment of regulated entities against typically established requirements • issuing common security guidelines, recommendations, or principles for institutions to follow • regulation on the basis of incident reports received from financial institutions.
Proactive regulation	• monitoring of IT processes for indicators of potential security risks • the implementation of new processes and prioritisation of resources in identifying and addressing possible risks or vulnerabilities arising out of the use of existing or new technologies • creating and building awareness on security risks • regular and timely exercises to identify threats which may later pose risks • providing recommendations and supervision to financial institutions based on potential risks identified.

Table 3-1 *Proactive and Reactive Regulation in the Financial Services Sector*

3.8 Criminal Liability and Responsibility

Some scholars have argued that government intervention through sanctions are arguably the most significant mechanism for sanctioning firms to implement standards which they have adopted on paper.[173] In this regard, risk management requires taking into account several factors including legal frameworks which regulate the interdependence of institutions, their

[173] Andrew A King and Michael J Lenox, 'Industry Self-Regulation without Sanctions: The Chemical Industry's Responsible Care Program' (2000) Academy of Management Journal 698, 702.

mandates and obligations, and coordination instruments like self-imposed standards[174] and incentives[175].

The distinctive goal of criminal law is the regulation of behaviours and conduct using the threat and imposition of punishment and consequences for contraventions. In the context of institutions therefore, responsibility will be attributed for contravention of the law, where it is found that their actions or inactions had resulted in a cyber security breach, contrary to the provisions of the law. Deterrence and Retribution have for a long time been recognised as the two common justifications for punishment under criminal law.

Retribution is a reactionary rationale for punishment involving a consideration of the events surrounding the offence committed, the accused's responsibility for the offence and on that basis determining the respective punishment for the relevant conduct. Two common aspects to the recognition of retribution as a goal of punishment is revenge which defends the imposition of punishments on the offender proportionate to the wrong suffered[176] and just deserts which focuses on rebuilding of the law and public morality and the idea that the perpetrator should recompense the public/society for the harm suffered.[177] However, the retribution model has been criticised as been largely complicated as it is founded on the concept of just deserts,[178] an excessively idealistic concept which speculates the existence of a just society in a world where resources are unevenly distributed.[179] Indeed, the just deserts theory as a natural justification for punishment is merely retrospective, does not concern itself with the realisation of future benefits such as the prevention of further crime, but only on imposing punishment appropriate to the harm suffered.[180]

---

[174] Renn, *Risk governance: coping with uncertainty in a complex world,* 9.
[175] For example, threats of punishments and consequences, usually regarded as negative incentives or recognition for implementation of best practices which may be regarded as a positive incentive due to the reputational impact.
[176] Gerben Bruinsma, Henk Elffers and Jan De Keijser, *Punishment, Places and Perpetrators* (Routledge 2012) 101.
[177] Monica M Gerber and Jonathan Jackson, 'Retribution as revenge and retribution as just deserts' (2013) 26 Social Justice Research 61, 63.
[178] Gerald A MacHugh, 'Christian faith and criminal justice: Toward a Christian response to crime and punishment' (1978) 101 in James M Day, *Crime, values, and religion* (Greenwood Publishing Group 1987) 71.
[179] Glenn D Walters, *Foundations of Criminal Science: The development of knowledge*, vol 1 (Greenwood Publishing Group 1992) 211.
[180] Kevin M Carlsmith, John M Darley and Paul H Robinson, 'Why do we punish? Deterrence and just deserts as motives for punishment' (2002) 83 Journal of personality and social psychology 284, 285.

Retribution is arguably not an effective as a basis for criminal enforcement, particularly in the context of the objectives of this research. Simply put, retribution is not an effective or sufficient justification for the punishment of a financial institution which has just been hit by cyberattacks. The purpose of the sanctioning framework/regimes is to essentially ensure that next time the financial institutions ensure that their systems are more resilient and this cannot be attempted or achieved by retribution. A great substitute to retribution/retributive justice is restorative justice which encompasses a set of criminal justice models and practices that view crime as a relationship problem and ensure justice by way of a constructive communication between victims, perpetrator and their societies with the aim of identifying moral obligations, to fulfil that which is required and remedy the harm inflicted.[181]

A theory which finds a common ground between the restorative and retributive justice models is the communicative theory of punishment proposed by Antony Duff[182] that regards punishment as an informational process which communicates to perpetrators the punishment that is fitting for their crimes and intends to encourage them to atonement, reformation and reconciliation.[183] While the communicative theory is applauded for its communicative purpose, Wringe has argued that it cannot be generalised. He maintained that while the account directs the imposition of legal punishment on individuals, some of the actors which the imposition of legal punishment may also be directed at include organisations and nations, which the theory does not cover and that a gap exists in the notion that punishment should be targeted at producing 'regret or remorse' and justified on the basis of reasons which reveal that the 'regret or remorse' felt by the individual possesses some sort of benefit.[184] Based on this, he argues that a "denunciatory" account of the punishment of organisations is needed to close this gap to allow for communication of the punishment to a larger audience, as opposed to communication to the perpetrator which Duff proposes.[185] The objective of the denunciatory account is to communicate to law-abiding persons that the

[181] Theo van Willigenburg, 'Restorative justice as empowerment: how to better serve the goals of punitive retribution' (2018) 1 International Journal of Restorative Justice 274, 282.
[182] James Dignan, *Understanding victims and restorative justice* (McGraw-Hill Education (UK) 2004) 104.
[183] Antony Duff and Robert Alexander Duff, *Punishment, communication, and community* (Oxford University Press, USA 2001) 89.
[184] Bill Wringe, 'Collective agents and communicative theories of punishment' (2012) 43 Journal of Social Philosophy 436, 438.
[185] ibid 443.

denounced conduct is unacceptable and recognises that individuals make up institutions and in the punishment of institutions, individuals are indirectly affected.[186]

In some ways, the denunciation and deterrence theories of punishment are quite alike in that they both aim to minimise the occurrence of crimes by using punishments as a tool to influence public perception, consider the essential function of sanctions as passing across information to the general public. In other ways, they are different as while the objective of deterrence is to drive budding offenders into desisting from wrongdoing by causing them to fear that sanctions may be imposed if they engage in wrongdoing, denunciatory punishments aim to reinforce and enhance the existing moral beliefs of people who supposedly have regard for the law-abiding principles.[187] This thesis shall not attempt a full-scale examination of the theories punishment of as this would, largely, require wider considerations of scholarly pieces and empirical evidence whose justification is falls outside the scope of this research. For the purpose of this research however, we will focus only on the principle of Deterrence.

Deterrence is essentially a precautionary approach to punishment; it is forward-looking and preventive in nature. To put in context, it entails punishment for a breach of cyber security requirements as a mechanism for preventing a firm from repeating the action/inaction that led to a cyberattack and inciting other firms to build defences against cyber threats/attacks and thus, achieving a preventive effect and strengthening resilience, usually conceived as a principal objective of any cyber security policy or system. For example, imposing substantially higher fines as punishment for breaching mandatory reporting requirements, inadequate data protection systems and infrequent cyber security threat assessments. Deterrence is conceived as the main underlying objective and rationale for attribution institutional criminal liability. It has been argued that because it is impossible to detain or execute a firm, any sanction imposed against it, must be one which possesses a deterrent effect.[188] This, as a claim, is what we seek to validate by analysing the form of criminal sanctions which may be imposed by the countries in our case studies for breaches of

[186] ibid 445.
[187] Matthew H Kramer, *The ethics of capital punishment: A philosophical investigation of evil and its consequences* (OUP Oxford 2011) 157.
[188] John B McAdams, 'The appropriate sanctions for corporate criminal liability: An eclectic alternative' (1977) 46 University of Cincinnati Law Review 989, 993 - 994.

cyber security legislation and regulations. This section will examine how these sanctions apply in the context of self-regulation and to understand if these sanctions may effectively induce institutional proactive cyber defences i.e., the deterrent effect.

The scope of organisational liability remains a subject of academic debate. While organisations may be held liable for a crime by virtue of provisions in legislation, issues often arise where the offence requires an element of a guilty mind to determine culpability. While an organisation may not be said to possess a guilty mind, its agents i.e., individuals who make up its decision-making units, however, may possess a guilty state of mind which may be associated with the organisation, such that the organisation itself may be held liable for the offence. This supports the argument that "Institutions are [mentally] constituted by individuals [who are also] socially constituted by institutions".[189] A detailed discussion of about this is outside the scope of this chapter, however, it is also closely linked with imposing liability on directors for corporate fault.

The above argument also echoes a long-standing argument over the creation of specific duties of care on firm Directors in statutes as an incentive to ensure there are adequate compliance systems.[190] To this end, it is argued that they automatically carry out that duty subject to the provisions of the statute. The first problem with this is that it encourages box-ticking and reactive behaviours. Also, with cyber security, measuring the adequacy of compliance systems by following a legislative checklist which places a duty of care on only directors fails to not only consider the dynamics of cyber security requiring co-ordination among other designated individuals, but also the need for proactive responses as the compliance system may be adequately set relative to existing threats, but not future ones.

An institution may also be held criminally liable where it takes steps explicitly or implicitly resulting in a cyber-attack in a bid to protect associated values. In this regard, we consider the Rational Actor Model (Model I), which presupposes that the way to criminalise the conduct of an institution is to consider the rational values behind the conduct. This suggests that sanctions imposed upon the firm may be effective if connected to values such as

[189] Brent Fisse and John Braithwaite, 'The allocation of responsibility for corporate crime: Individualism, collectivism and accountability' (1986) 11 Sydney Law Review 468, 478.
[190] Margot Priest, 'The privatization of regulation: five models of self-regulation' (1997) 29 Ottawa Law Review 233, 294.

profit or sales maximisation and reputational advantage.[191] Applying this model in the context of a cyber security breach, a fine imposed upon a financial institution for the period of the breach could be a sum of all profits made during the period of the breach (in addition to the cost of compensation for losses experienced by customers). Similarly, such sanctions could extend to reputational advantages by regulators issuing public notices or reports on banks found to be in breach of cyber security requirements.

In contrast with Model I, Kriesberg also proposes an Organisational Process Model (Model II) which recognises the existence of various decision-making units/processes and the results which emanate from a structure of divided controls and conventional practices.[192] In the context of our research, it implies that liabilities arise where standard operating procedures permit or authorise cyber security failures. Thus, liability should be imposed upon units whose roles include cyber security reporting, implementing and overseeing adequate cyber security standards etc. However, the efficiency of departmental sanctions under Model II may be arguable where it encourages reactive responsibility-taking and also because cyber security is a collective responsibility across a number of individually connected responsibilities. The uncertainty of this model is also reflected in its lack of clarity as to the subject(s) of the sanction i.e., an institution or an individual, as opposed to a unit.[193] Mellema partly supports this argument, highlighting the uncertainty that arises from imposing collective responsibility on an institution for failures/hazards noting that it overlooks individual responsibility for actions or inactions leading to the incident and undermines the ethics of moral responsibility.[194] However, Isaacs and Vernon disagree and argue that collective responsibility possesses significant implications especially for regulatory outcomes such that justice might be served through various methods of accountability[195] and the outcomes could be more effective than pursuing individual responsibility which is often times resource consuming.[196]

---

[191] Simeon M Kriesberg, 'Decisionmaking models and the control of corporate crime' (1976) 85 Yale Law Journal 1091, 1106 - 1107.
[192] ibid 1112 - 1114.
[193] ibid 1115.
[194] Gregory Mellema, *Collective responsibility*, vol 50 (Rodopi 1997) 38.
[195] Such methods include public disclosures and reports, performance assessments, monitoring the implementation of regulatory guidelines and policies etc.
[196] Tracy Isaacs and Richard Vernon, *Accountability for collective wrongdoing* (Cambridge University Press 2011) 7.

Feinberg expresses a combination of enthusiasm and caution for model of the collective responsibility suggesting that its application of hinges on flexible forms of 'social blame', on the basis of fairness rather than strict liability and notes that application is to be determined on a case-by-case basis taking into account factors such as different extents of individual involvements, with varying levels of initiative, significance of designated duties, positions of authority, etc.[197] Overall, systems of collective responsibility have been argued to incentivise change between groups and shape future conducts.[198] They potentially offer a starting point for institutional reforms, in instances where collective actions have been previously neglected.[199]

In an alternative approach drawn up from Fisse[200], an institution can be criminally liable for: (i) providing 'a policy that expressly or impliedly' facilitates or allows the materialisation of a cyber-attack; (ii) 'failing to exercise due care and diligence' to prevent the materialisation of a cyber threat or attack; (iii) 'failing to comply with a reactive duty' to take proactive measures in response to a notice/warning of addressing inadequate security controls; or (d) failing to implement necessary safeguards to comply with a reactive obligation to carry out precautionary measures in addressing already identified security breaches, or failing to implement 'reasonable' safeguards or to exercise 'due diligence', through action or inaction.

The relevance of establishing criminal liability is reinforced by the Bank of England's Written Evidence to the Wilson Committee in connection with stage two of its inquiry, noting: "that non-statutory arrangements *combined with statutory provisions* will continue to provide an effective and flexible system of control."[201] Indeed, self-regulatory structures are dependent on existing statutory structures to the extent that the latter elaborates a salient enforcement structure within it for the purposes of monitoring and correction.

The likely self-regulation success factors highlighted in the findings of Priest accentuate the importance of punishment for breaches/unlawful conduct in realising

[197] Joel Feinberg, 'Collective Responsibility' (1968) 65 The Journal of Philosophy 674, 687.
[198] Christian List and Philip Pettit, *Group agency: The possibility, design, and status of corporate agents* (Oxford University Press 2011) 157 - 168.
[199] Marion Smiley, 'Collective responsibility' (2005) Section 6.
[200] Brent Fisse, 'The attribution of criminal liability to corporations: A statutory model' (1991) 13 Sydney Law Review 277, 279.
[201] Bank of England's Written Evidence to Wilson Committee in connexion with Stage Two of its Enquiry: 'Regulation in the City and the Bank of England's role', QB (1978) Q3, p 382, para 26.

regulatory objectives.[202] In firm-defined regulation, offences (regulatory, civil, and criminal) may be found in legislation which are considered a last resort, following the failure of private enforcement.[203] Examples include the destruction, erasure, modification and concealment of information to prevent disclosure[204] and reporting requirements for operators of essential services.[205] The table below summarises the features/advantages of self-regulation and the associated drawbacks in support of the need for regulation in the shadow of government intervention:

Advantages	Drawbacks
Flexibility: Rules can be modified on time to reflect the changing cyber threat landscape, compared to the lengthy process involved in amending government legislation.	Abuse of Discretion: As institutions enjoy regulatory flexibility, there is a possibility of using this discretion to avoid rigid forms of direct regulation that may affect its specific values and/or interests.
Less Costly: It may involve less costs to the government since the private sector is saddled with taking on the regulation of itself.	Oversight Costs: There may be increased costs in the event of a self-regulatory failure where direct regulation requires extensive monitoring and enforcement efforts.
Enhanced Compliance: There may be increased compliance levels due to the participation of the sector in developing regulation for itself, and by virtue of that assumes responsibility.	Feigned compliance: In relation to reporting obligations, there is the risk of institutions' feigning compliance and producing inaccurate records[206] which invariably presents a difficulty with establishing criminal liability and may only be detected through investigation by regulators.
Self-enforcement: There is increased involvement of the sector in enforcement of the rules which it creates since it is being delegated	Reduced Accountability: In the absence of regular checks on conduct, accountability may sometimes be lost as the government when

[202] Priest, 'The privatization of regulation: five models of self-regulation' 239.
[203] ibid 244.
[204] Data Protection Act 2018, Section 173.
[205] Network and Information Systems Regulations 2018, Regulation 11.
[206] Fisse, 'The attribution of criminal liability to corporations: A statutory model' 296.

by the government to carry out some of its functions and, as such, is in possession of certain delegated powers.	directly exercising these powers is often subject to judicial review, ministerial responsibility etc.[207]

Table 3-2 *Advantages and Disadvantages of the Self-Regulation Approach*

Institutional liability ". . . is veil piercing at its most extreme in the sense that any protective corporate veil of the business entity is nigh on invisible as regulation surrounds individual employees, officers and contractors of the regulated entity; seeks to shape their conduct; and where necessary, wields its stick through sanction and discipline."[208] The chart below shows the type of government sanctions which may be applied, where institutions fail to effectively self-regulate:

Figure 3-1 *Government Sanctions for Self-Regulatory Failures*

Fines: These are the most common penalty imposed for the commission of a crime. The amount imposed may vary depending on the circumstance. They may also include orders to pay compensation to victims. For instance, if a bank loses £300,000 of customer funds to a hacker during a cyber-attack, a regulator may levy a fine against it where it finds that it had

[207] Priest, 'The privatization of regulation: five models of self-regulation' 273.
[208] Gray Joanna and Hamilton Jenny, *Implementing Financial Regulation-Theory and Practice* (Wiley Online Library 2016) 70.

failed to exercise due diligence to prevent its IT system failure, and may also be ordered to pay compensation/issue refunds to customers affected by the attack.

This confirms the notion that sufficiently high costs of liability may incentivise a change of conduct both in individuals and firms.[209] That is, the higher the costs of potential liability, the more likely it is to achieve a deterrent effect due to the fact that fairness/proportionality of punishment prescribed to firms' is then overridden by fairness to the public, such that they are then held up to a much higher standard. Nevertheless, to argue that higher fines have a high likelihood of a deterrent effect is a debatable claim, especially in instances of a calculated risk where the institution involved considers the cost of implementing adequate cyber security systems to be higher than the cost of punishment or where the cost of punishment is reduced or cleared due to social/political ties.

Fines may also be mitigated where a firms' responsibility to exercise reasonable care and due diligence to provide adequate security controls can be proven. For instance, some regulators may considerably deduct from or discount fines levied against firms by considering a wide range of factors including the nature of the breach, timing of the breach, impact/likely impact of the breach, profits gained/losses averted and losses to consumers.[210] This indicates how the "passive" accountability by way of public sanctioning of responsibility undergoes revisions and adjustments to incentivise and encourage a further "active" sense of responsibility in stimulating more engaged and ideal management that will accept the responsibility for effective regulation within the firm.[211] However, while fines may incentivise financial institutions to produce structures for practising due diligence, they may not necessarily produce learning and accountability. Will learning be achieved where a financial institution's agent responsible for operational decision making, has been reckless or negligent in their duty? Should there not be separate internal disciplinary sanctions or external interventions for the attribution of responsibility?

Bad Publicity: Considered as the most likely underrated sanction, bad publicity is regarded as being effective for punishing corporations and deterring future unlawful

[209] Priest, 'The privatization of regulation: five models of self-regulation' 293.
[210] Financial conduct Authority, 'FCA Handbook, DEPP' Chapter 6 <https://www.handbook.fca.org.uk/handbook/DEPP/6.pdf> accessed 9 February 2020.
[211] Joanna and Jenny, *Implementing Financial Regulation-Theory and Practice*, 110.

conduct.[212] Bad publicity is often triggered by legal sanctions and is rarely used by itself.[213] Indeed, bad publicity is often the by-product of legal sanctions in which reports, notices and warnings issued regarding a firms' unlawful conduct are made public. These are often persuasive in nature and may result in a potential change in behaviour, for the fear of absolute reputational damage and loss of customer confidence.

Corrective Actions: These are cyber security actions or requirements which firms have to implement promptly as a result of the investigations by and settlements with regulators to enhance existing cyber security practices and mitigate against IT system vulnerabilities such as compliance control issues, data compromise, network disruptions and system intrusions.

In summary, the interpenetration between government actors and sectoral actors may comprise of a stringent or flexible monitoring partnership or direct imposition alongside sanctions by the former against the later in instances of a breach for positive or negative incentivisation, facilitating lawful conduct, stipulating procedural rules etc.[214] If requirements are imposed and combined with sanctions, they may produce greater sector regulatory effectiveness, subject to policy considerations.[215] Financial institutions may therefore be able to effectively self-regulate, dependent however, upon governmental sanctions which may be imposed in the event of a cyber security breach either directly or indirectly, through specifically designated regulatory agencies.

3.9 Reflexivity in Practice: For Better or Worse?

Reflexivity as we have observed, appears to increase the potential for effectiveness in regulation. However, questions arise as to whether reflexivity always produces better regulation. While reflexive interactions and learnings between and within institutions may facilitate the production and reproduction of knowledge, in other cases, it may place constraints on regulation where relevant structures and functions are absent. Indeed, a

[212] R. Mokhiber, *Corporate Crime and Violence: Big Business Power and the Abuse of the Public Trust* (Sierra Club Books 1988) 59.
[213] C. Parker and Organisation for Economic Co-operation and Development, *Reducing the risk of policy failure: challenges for regulatory compliance : final version* (OECD 2000) 70.
[214] Héritier and Lehmkuhl, 'The shadow of hierarchy and new modes of governance' 2.
[215] ibid 3.

developing country adapting the regulatory frameworks of a developed country does not automatically guarantee success, effectiveness or even sustainability. Pillow explores the objective of reflexivity and questions whether one can certainly represent another's posture, if representation should be the objective and if the story is then that of the "researcher or researched".[216] To rephrase Pillow's question, we question whether one country can successfully represent the narrative of another, especially where the surrounding context of the country being modelled, and the country modelling are significantly different. Merely adopting rules is not actual representation, as without knowledge of specific circumstances, there can be no effective implementation.

Is reflexivity possible without readjusting norms, values, structures, or analysing data? Maybe not. While reconstruction with little or no facts may facilitate broad changes to the system, the lack of data blurs understanding of the target risks, and ultimately restrains effectiveness of frameworks. Without evidence, there is no justification of processes, and reflexivity may not be argued to be useful. The usefulness of reflexivity lies in the nature of its transparency, self-referentialism, interdependence, accountability, criticality, flexibility, introspectiveness, retrospectiveness and prospectiveness. However, factors like inadequate training, insufficient funding and resources, political interference, weak disciplinary systems, and structural chaos, tend to stir reflexivity towards the worse.

Better reflexivity focuses on the foundation (why), structure (what) and maintenance (how), and not merely on the structure. Unfortunately, some regulatory frameworks do not implement a holistic approach towards the management of cybersecurity risks. Sometimes, a structure might be present without a foundation, and even where the foundation and structure are present, maintenance is often inadequate. Maintenance should be instructive; setting out detailed guidelines to direct and influence operations, preventive; regularly monitoring and supervising operations to ensure continuous resilience, and corrective; intervening in the event of an IT system failing where due diligence practices have been followed or not and imposing fines and/or sentences.

[216] Wanda Pillow, 'Confession, catharsis, or cure? Rethinking the uses of reflexivity as methodological power in qualitative research' (2003) 16 International journal of qualitative studies in education 175, 176.

Where a country draws lessons from a model which is inherently problematic, in the absence of thorough applicability assessments, there is a risk that any lessons learned will be most likely unworkable. Meanwhile, even where lessons are drawn from an effective model, reflexivity may not automatically guarantee attainment of policy objectives if functions have not been well-defined.

In summary, reflexivity may not always be something to strive towards where there is no orientation highlighting advantages and disadvantages of the model frameworks, towards ensuring successful navigation of the adaption process.

3.10 Conclusion

It appears undoubtedly true that in a reflexive model of regulation, lines between government and private regulation are somewhat blurred where regulation operates both as an informative and normative tool to manage the occurrence and prevent the reoccurrence of mistakes, but also to influence behaviour, enforce accountability and ensure policy objectives are achieved.

Particularly, in respect of cybersecurity, there is the need for regulations and laws in the background which impose standards on FIs to take reasonably necessary steps processing customer information and transactions, conducting its operations and its management overall. On the foreground, rules, guidance and policy documents are to be issued setting out cybersecurity best practice requirements for institutions to take into account when developing internal policies. This is to be backed, however, by regular supervisory and monitoring arrangements in which regulators may carry out assessments on the effectiveness of policies in place as well as compile records of existing, new or potential issues of security concern which will serve the purpose of "revisability of [strategies] in the [mitigation] of side effects [which may be] discovered later."[217]

It is, of course, possible for firms to be reluctant to effectively regulate their business operations, despite having the capabilities to do so.[218] Where this happens, regulators may ward off this voluntary self-regulation curse through legal intervention by conducting

[217] Beck and others, *Risk Society: Towards a New Modernity*, 178.
[218] John Braithwaite, 'Enforced self-regulation: A new strategy for corporate crime control' (1982) 80 Michigan law review 1466, 1469.

investigations, imposing penalties, and mandating institutions to take corrective actions, where necessary. It is therefore important that indirect and direct regulatory instruments play an important role in regulation. An effective cybersecurity risk management framework is one which demands less state intervention, and intentionally focused on devising structures and arrangements which reflect the evolving cyber threat landscape and influences the conduct and understanding of financial institutions toward building their resilience capabilities.

Finally, where models are adapted with no justification of choices or evidence of effectiveness, no clear reflexivity is achieved, and a country must in that moment, develop its own internal and external structures and systems and draw upon its own conclusions.

Chapter 4. Case Study United Kingdom

4.1 Introduction

Both the concepts of "regulation" and "risk management" are rooted in reflexivity practices. That is, they facilitate the creation of cybersecurity frameworks which adapt not only criminal justice standards, but also self-regulatory norms. The implementation of effective cybersecurity risk management frameworks becomes increasingly important as evolving technologies continue to present cyber risks which the financial sector must regulate.

The Financial Conduct Authority (FCA) describes cybersecurity as "a combination of human and technology risks" posed to the sector[1], recognising risks arising from failing IT processes due to human actions, inactions or omissions. Such combined risks may take the form of network disruptions and data breaches, amongst others which have multiscale and sometimes far-reaching geographic impacts. For instance, the 2016 Tesco Bank cyberattack[2] resulting in a loss of £2.26 million of customer funds, and the 2017 Equifax data breach[3] resulting in the theft of personal data of 694,000 UK consumers, attracting fines of £16.4 million and £500,000 from the FCA and Information Commissioner's Office (ICO), respectively. The materiality of these cyber incidents prompts an evaluation of the cybersecurity risk management processes adopted in financial institutions and the difficult issue related to determining when legal interventions may be pursued in the event of self-regulatory failures.

In this chapter, we discuss the cyber risks trends in the UK's financial sector and their impact using findings drawn from the Annual Reports of Barclays Bank Plc and Lloyds Banking Group, two leading UK banks, and identify cybersecurity risk management processes adopted in both banks and whether these align with the objective of reflexivity. To

[1] Financial Conduct Authority, 'Cyber and technology resilience in UK financial services' (27 November 2018) *Speeches* <https://www.fca.org.uk/news/speeches/cyber-and-technology-resilience-uk-financial-services > accessed 13 August 2019.
[2] Financial Conduct Authority, 'Final Notice: Tesco Personal Finance Plc' (1 October 2018) <https://www.fca.org.uk/publication/final-notices/tesco-personal-finance-plc-2018.pdf> accessed 4 August 2019.
[3] Information Commissioner's Office, 'Credit reference agency Equifax fined for security breach' (20 September 2018) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/credit-reference-agency-equifax-fined-for-security-breach/> accessed 28 December 2020.

clearly demonstrate possible institutional or regulatory issues that may have forestalled the implementation of reflexive cybersecurity practices in the sector, we probe the efficacy of current sanctioning regimes employed by regulators, challenges surrounding effective regulation and examine the adequacy of cybersecurity legislation in the financial sector. In the same vein, we examine international, EU and national cybersecurity standards; with an in-depth look at the UK's Network and Information Systems Regulations 2018 and close with a review of factors inhibiting reflexivity in current cybersecurity risk regulation in the financial sector and highlight what could be done to overcome the problems.

4.2 Overview of the UK Institutional Framework

Between the years 1825 – 2008, the UK experienced a series of financial crises which threatened the stability of its financial system.[4] The financial crisis which brought about a significant change in the regulatory structure of the UK financial sector occurred in the year 2008. A major incidence in the course of the financial crisis was the fall of Northern Rock (NR) in 2007 which exposed major failings in regulation and supervision within the financial system. In particular, the Financial Services Authority's (FSA) Internal Audit Report highlights major issues such as a failure to assess NR's weak business framework, huge time gaps between review periods; ineffective identification of risk profile; inadequate supervisory expertise; and no meeting notes recorded for important consultations.[5] These issues which were argued to have arisen out of failure in the 'implementation of its regulatory responsibilities'[6] towards applying its ARROW framework appropriately to NR's risk rating, led to the abolishment of the FSA.

The crisis led to the introduction of three new bodies to be responsible for the regulation of the financial sector namely the Financial Planning Committee (FPC), the FCA and the Prudential Regulation Authority (PRA), which are examined in detail later in the chapter. Generally speaking, the challenges to regulation in the financial sector are now increased due to the risks posed by increasing reliance on computers, devices and networks.

[4] N.H. Dimsdale and A. Hotson, *British Financial Crises Since 1825* (Oxford University Press 2014) 1 - 5.
[5] FSA Internal Audit Division, 'The supervision of Northern Rock: A Lessons Learned Review Report' (March 2008) para 26 <https://www.fca.org.uk/publication/corporate/fsa-nr-report.pdf> accessed 14 August 2019.
[6] M. Ariff, J. Farrar and A.M. Khalid, *Regulatory Failure and the Global Financial Crisis: An Australian Perspective* (Edward Elgar Pub. 2012) 170.

In the Bank of England *2019 H2 Systemic Risk Survey*, cyberattack was reported as the second largest threat to the UK financial system, after 'UK political risk'.[7] Indeed, firms reported 459 technology and cyber incidents in the sector in 2019.[8] The UK financial services sector regulates risks associated with technology using guidance which consists of cybersecurity practices as well as legislation and policies which institutions must take into account to enhance cyber risk management.

The primary approach to regulation in the UK financial services sector is the decentred approach, consisting of a system of self-regulation which considers law as a broader part of regulation. According to Black, such systems recognise that certain activities/conducts must be subject to certain values and appropriate objectives.[9] For instance, in the UK, both the FCA, the conduct regulator, and PRA, the prudential regulator, subjects the activities of institutions to the realisation of its statutory objectives.

In the UK, FIs are expected to adhere to several regulatory requirements and consider numerous guidance and reports issued to provide standards which may be implemented for best cybersecurity practices. Examples of such guidance and reports include the Bank of England's Financial Stability Report,[10] the FCA's Senior Management Arrangements, Systems and Controls Sourcebook[11] and the FCA's Cybersecurity Guidance.[12] This issuance of guidance has been highlighted by Galligan as the implementation of regulation through which the conducts of firms are influenced, other than directly interfering with conduct or imposing threats of sanctions.[13]

[7] Bank of England, 'Systemic Risk Survey Results - 2019 H2' (16 December 2019) <https://www.bankofengland.co.uk/systemic-risk-survey/2019/2019-h2> accessed 31 December 2020.
[8] Financial Conduct Authority, 'Sector Views 2020' 13 <https://www.fca.org.uk/publication/corporate/sector-views-2020.pdf> accessed 28 December 2020.
[9] Black, 'Critical reflections on regulation' 28.
[10] Bank of England, 'Financial Stability Report Issue 37' (July 2015) <https://www.bankofengland.co.uk/-/media/boe/files/financial-stability-report/2015/july-2015.pdf> accessed 28 December 2020.
[11] Financial Conduct Authority, 'SYSC 3 System and Controls' <https://www.handbook.fca.org.uk/handbook/SYSC/3/1.html> accessed 28 December 2020.
[12] Financial Conduct Authority, 'Good Cybersecurity - The Foundations' (22 June 2017) <https://www.fca.org.uk/publication/documents/cyber-security-infographic.pdf> accessed 28 December 2020.
[13] Galligan, *Law in modern society*, para 8.5.

The model of regulation adopted in the UK is the twin-peaks model approach, a regulatory arrangement involving regulation by objective[14] and requiring a separation of regulatory roles between regulators, such that each objective is the responsibility of a separate regulator.[15] The regulation of cyber risk in the financial sector in the UK is undertaken by three primary authorities as represented in the chart below:

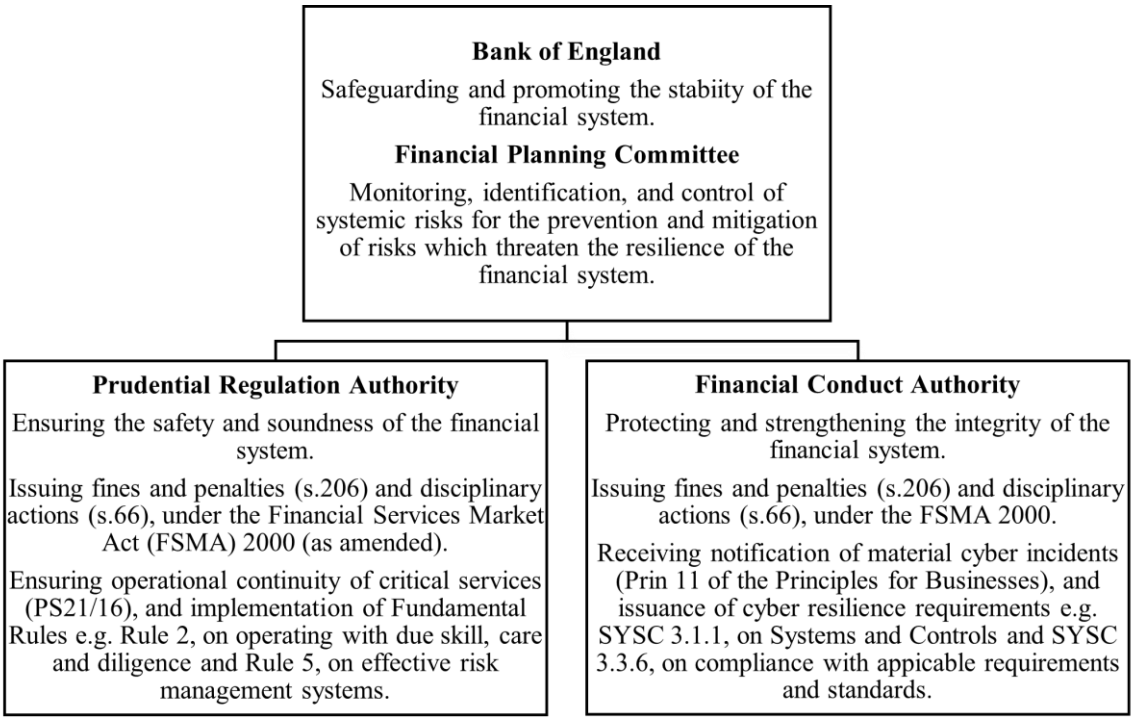

Figure 4-1 *UK Financial Regulatory Approach to Cyber Risk Regulation*

[14] "an objective-oriented approach", see Eilis Ferran, 'The break-up of the financial services authority' (2011) 31 Oxford Journal of Legal Studies 455, 464.
[15] Andrew Godwin, Timothy Howse and Ian Ramsay, 'A Jurisdictional Comparison of the Twin Peaks Model of Financial Regulation' (2017) 18 *Journal of Banking Regulation* 103, 105 <https://ssrn.com/abstract=2905458> accessed 9 March 2018.

Financial Planning Committee

The FPC was an interim body initially set up by the BoE's Court of Directors[16], and subsequently established as an independent body with statutory powers by virtue of the FSA 2012, primarily for the purpose of contributing to the BoE's effort in achieving its objectives.[17]

As part of its financial stability objective, the committee is also authorised 'to give directions or make recommendations'[18] to the FCA or PRA in relation to their regulated entities. Thus, the FPC possesses the veto power to give directions on systemic issues.[19] For instance, in its Financial Stability Report, the FPC provides cyber-related directions by detailing the structure of its pilot cyber stress tests, including critical vulnerability scenarios to be considered towards developing effective response plans.[20]

Prudential Regulation Authority

The PRA and the FCA were established in 2013 in accordance with Part 1A of the FSMA 2000[21], the legislation which brought the supervision of the financial sector under the FCAs predecessor, the Financial Services Authority (FSA).

As part of its threefold regulatory and supervisory objectives, the PRA is to ensure that the activities of its regulated entities are not conducted in a way that results in 'adverse effect on the stability of the UK financial system and to take steps to mitigate the adverse effect that the failure of its entities may bring about'.[22] By virtue of its mandate, the PRA has

[16] Bank of England, 'Financial Policy Committee' <http://www.bankofengland.co.uk/financialstability/Pages/fpc/default.aspx> accessed 8 September 2017
[17] Financial Services Act 2012, Section 9C(1a).
[18] Financial Services and Markets Act 2000, Section 9H and 9Q.
[19] Great Britain: Parliament: House of Commons: Treasury Committee and A. Tyrie, *Financial Conduct Authority: twenty-sixth report of session 2010-12, report, together with formal minutes, oral and written evidence* (Stationery Office 2012) para 97.
[20] Bank of England, 'Financial Stability Report Issue No. 45' (July 2019) <https://www.bankofengland.co.uk/-/media/boe/files/financial-stability-report/2019/july-2019.pdf?la=en&hash=976688AB50462983447A8908BE079743A3E3905F> accessed 26 December 2020.
[21] As amended by the Financial Services Act 2012.
[22] Bank of England, 'Memorandum of Understanding: Between the Financial Conduct Authority and the Bank of England (exercising its prudential regulation functions)' (July 2019) para 10 <https://www.bankofengland.co.uk/-/media/boe/files/memoranda-of-understanding/fca-and-bank-prudential-july-2019.pdf?la=en&hash=8DE71C08C48852C15DB5A999A74B95D48B507F16> accessed 4 August 2019.

in recent times exercised its enforcement powers in the regulation of cyber risks as a joint collaboration with the FCA, thereby indicating its willingness to mitigate any such risks which threaten the stability of the financial system.[23]

Financial Conduct Authority

To achieve its objectives under the Financial Services and Markets Act (FSMA) 2000, the FCA is required to have regard for the stability, soundness, and resilience of the financial system towards ensuring that it is not being used as a conduit for financial crime. In effect, the FCA has a role in the regulation of cybercriminal conducts as attacks on financial systems and networks are often widespread undermining the resilience, soundness and stability of the sector. This role involves, collaboration with the BoE to review the resilience of major FIs, performance of risk-based cybersecurity assessments on large institutions, running a communications plan to offer assistance and guidance on nationwide security standards for small institutions and typically, providing the initial response and cooperating with other authorities, e.g. Her Majesty's Treasury, the BoE, PRA etc, where there is a material cyber incident affecting the sector.[24]

Regulation by the PRA and FCA is integral to the financial services sector and both authorities coordinate and cooperate to assist institutions to evaluate their cyber resilience capabilities by dual-developed self-assessment operational resilience questionnaires.[25] FIs which the PRA supervises and prudentially regulates are also subject to the FCA's conduct regulation, hence they consult with one another on policy considerations such as enhancing operational resilience of its institutions and the market, or recommending institutions to set an impact tolerance level for their operations, calculating the highest acceptable level of disruption through extreme, but highly likely situations.[26] This recommendation echoes the

[23] See Bank of England, 'R. Raphael & Sons plc – Final Notice' (29 May 2019) <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/regulatory-action/r-raphael-and-sons-plc-final-notice-may-2019.pdf?la=en&hash=CA2EDBA1E3FA560F6E22BA13C8B7CBA8676B1FA4> accessed 31 December 2020.
[24] Financial Conduct Authority, 'FCA Mission: Our Approach to Supervision' (March 2018) 11 <https://www.fca.org.uk/publication/corporate/our-approach-supervision.pdf> accessed 31 December 2020.
[25] Financial Conduct Authority, 'Cyber Resilience' (18 May 2017) <https://www.fca.org.uk/firms/cyber-resilience> accessed 4 December 2020.
[26] Bank of England, 'Building operational resilience: Impact tolerances for important business services' (5 December 2019) para 1.13 <https://www.bankofengland.co.uk/-/media/boe/files/prudential-

argument in Chapter 3 on acceptable risk levels and brings into view Beck's suggestion that accepting any risks at all, must be accompanied by well-defined limits. While the decision on setting tolerance levels is left to institutions, the supervisory authorities note that implementation is to be supervised and that regular assessments must be carried out to identify constraints on the institution's capacity to continue within the set tolerance levels and to strengthen its operational resilience.[27] As these are merely proposals, there is much left to be streamlined in the requirements/expectations, and though there is a reasonable need to protect the financial sector from over-regulation, concerns arise as to whether such critical decisions should be wholly left to the institutions.

4.3 Emerging Risk in the UK Financial Sector

Prevalent Cybercrimes in the UK Financial Sector

According to the Economic Crime Strategic Board (ECSB), the total fraud volume loss in the UK continues to rise exponentially, with 86% of fraud reported being cyber-enabled.[28] UK Finance estimates fraud losses due to unauthorised internet and mobile banking for the year 2018 at £130.9 million.[29] The advancement of technology has offered cyber criminals various opportunities to defraud unsuspecting victims of their money.

The FCA highlights ransomware, malicious insider threats, social engineering attacks and credential stuffing as current cyber threats facing the financial landscape.[30] In its cross-sector survey on cyber and technology resilience, it also emphasises third party risks as the second highest major cause of operational cyber incidents[31] and observe that FIs encounter

---

regulation/consultation-paper/2019/building-operational-resilience-impact-tolerances-for-important-business-services.pdf?la=en&hash=DAD20B3E08876E418863D37A242214BB1F32FE0A> accessed 4 August 2019.

[27] Bank of England, 'Building operational resilience: Impact tolerances for important business services' para 1.16.

[28] National Crime Agency, 'Public Private Threat Update Economic Crime - Key Judgements' (July 2019) <https://nationalcrimeagency.gov.uk/who-we-are/publications/323-public-private-threat-update-2019-economic-crime/file> accessed 2 August 2019.

[29] UK Finance 'FRAUD THE FACTS 2019: The definitive overview of payment industry fraud' 33 <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf> accessed 2 August 2019.

[30] Financial Conduct Authority, 'Insights from the Cyber Coordination Groups' (11 March 2020) <https://www.fca.org.uk/publications/research/insights-cyber-coordination-groups> accessed 20 December 2020.

[31] Financial Conduct Authority, 'Business Plan 2019/2020' 16 <https://www.fca.org.uk/publication/business-plans/business-plan-2019-20.pdf> accessed 4 August 2019.

cyber vulnerabilities in areas of people, third-party management, and key infrastructure safeguards.[32]

Scale and Impact of Cyber Risks

In the 2019 H1 *Systemic Risk Survey* by the Bank of England, 60% of respondents highlighted cyber-attack as source of risk to the financial system (a 6% decrease from the 2016 H2 survey).[33] Likewise, in the *UK Finance Fraud the Facts* report, cyber-related risk trends were seen to have resulted in significant losses for the sector. The total losses as well as total fraud volumes across years 2017,[34] 2018[35] and 2019[36] are represented below.

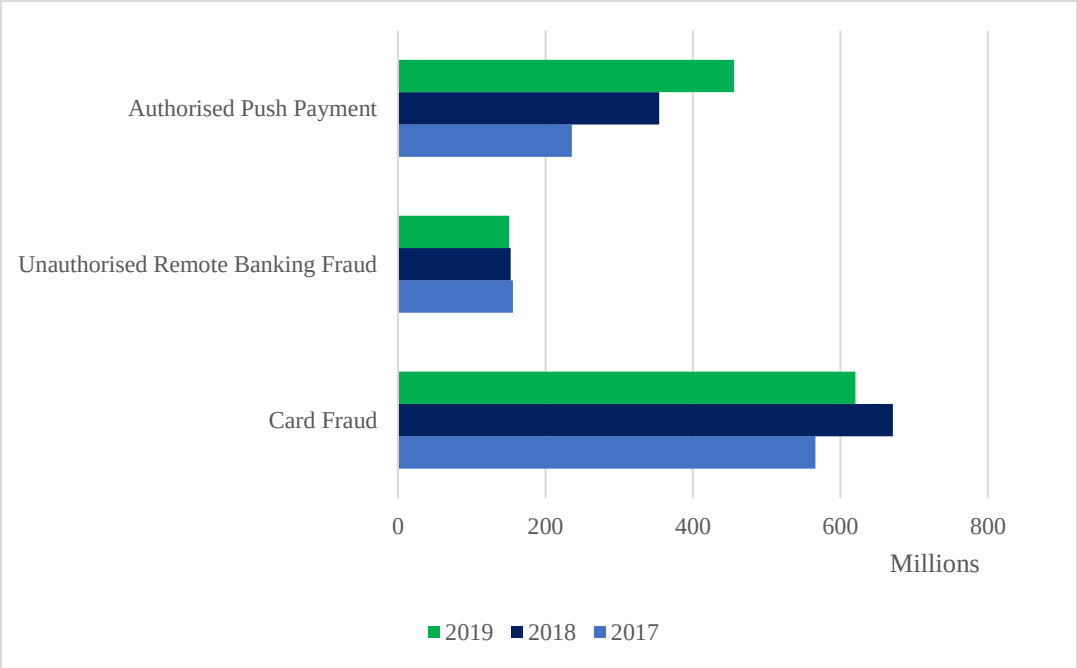

***Figure 4-2** UK total fraud losses by crime, 2017 – 19*

[32] Financial Conduct Authority, 'Cyber and Technology Resilience: Themes from cross-sector survey 2017/2018' (November 2018) para 2.4 <https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf> accessed 6 August 2019.
[33] Bank of England, 'Systemic Risk Survey Results - 2019 H1' (11 July 2019) <https://www.bankofengland.co.uk/systemic-risk-survey/2019/2019-h1> accessed 9 August 2019.
[34] UK Finance 'FRAUD THE FACTS 2018: The definitive overview of payment industry fraud' (31 July 2018) <https://www.ukfinance.org.uk/system/files/Fraud%20the%20facts-%20August%202018.pdf> accessed 28 May 2020.
[35] UK Finance 'FRAUD THE FACTS 2019: The definitive overview of payment industry fraud' (21 March 2019).
[36] UK Finance 'FRAUD THE FACTS 2020: The definitive overview of payment industry fraud' (14 May 2020) <https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-14-May.pdf> accessed 28 May 2020.

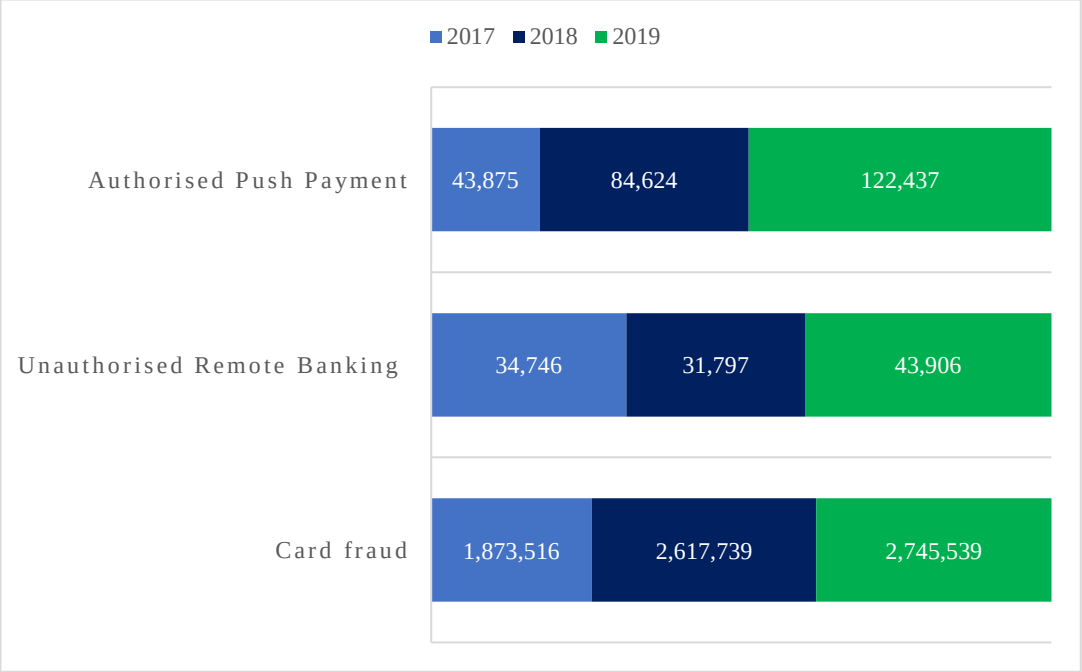

***Figure 4-3** UK total fraud case volume by crime, 2017 - 19*

The total losses on cards issued in the UK for the year 2019, amounted to an 8% decrease from the estimated figures in 2018 which may be partly due to the heightened security authentication introduced in September 2019 for e-transactions of significant value.[37] This decrease may also arguably be attributed to other fraud prevention mechanisms such as: sharing intelligence through the Financial Intelligence Hub; collaboration with law enforcement and other government partners; behavioural biometrics; fraud screening recognition devices;[38] real-time data analysis; and the engagement of a specialist police unit to disrupt the activities of organised criminal gangs.[39] Indeed, a decrease in the total losses compared against a 5% rise in the total case volume[40] for the year 2019 suggests that efforts are being made throughout the sector in the prevention of fraud. Meanwhile, victims of this

[37] UK Finance 'FRAUD THE FACTS 2020: The definitive overview of payment industry fraud' (14 May 2020) 13.
[38] For example, 3D Secure technology.
[39] UK Finance 'FRAUD THE FACTS 2020: The definitive overview of payment industry fraud' (14 May 2020) 13.
[40] That is, number of accounts defrauded.

type of fraud are protected under the law[41] against losses and often receive compensation for their losses.

In ***Figure 4-2***, the total fraud loss in this category for the year 2019 shows a 1% decrease from the year 2018 as well as a 38% rise in the case volume across the same years. The increasing case levels may be explained not only by the growing number of e-banking customers,[42] but also by an increase in fraud reporting, and possibly fraud detection. The decrease, on the other hand, may be attributed to the use of biometric authentication, collaboration with key actors, intelligence/information communication, implementation of security software and education and awareness programs for customers.[43]

For Authorised Push Payment (APP) fraud, the total losses for the year 2019 show a 29% increase from the year 2018 and a 45% increase in overall case volume across same years. The increase in the case numbers and losses may be partly due to the means by which the stolen funds are moved i.e., the criminal transfers the money into several accounts (usually controlled overseas) for it to be withdrawn. As a result, such funds are rarely traceable by banks.[44] To address APP risks, the financial sector in partnership with Pay.UK are set to adopt new technology to help trace fraudulent transactions and detect criminal accounts. Meanwhile, with APP frauds, a customer may only be entitled to protection under the law if it is found that the APP fraud was as a result of issues with the bank or PSP and that a customer was compliant with standards set out in the Voluntary Code.[45] Other steps taken to address APP frauds include implementing recovery standards for scam victims and investing in the government programme to reform the Suspicious Activity Reports system.[46]

On the whole, while these figures haven shown that there are some improvements, they show that a lot still needs to be done – particularly if the total losses and prevented fraud

[41] For instance, the Payment Services Regulations 2009 and the Consumer Credit Act 1974 which provide protection for consumers where there has been a fraudulent/unauthorised activity on their account.
[42] UK Finance 'FRAUD THE FACTS 2020: The definitive overview of payment industry fraud' (14 May 2020) 35.
[43] ibid 36.
[44] ibid 45.
[45] Lending Standards Board, 'Contingent Reimbursement Model Code for Authorised Push Payment Scams' (28 May 2019) < https://www.lendingstandardsboard.org.uk/wp-content/uploads/2019/05/CRM-code.pdf> accessed 28 May 2020.
[46] UK Finance 'FRAUD THE FACTS 2020: The definitive overview of payment industry fraud' (14 May 2020) 47.

have similar figures. This simply means that the risk of cyberattacks in the banking sector progresses in an upward movement, more than any other sectors.

4.4 The Self-Regulatory Fundamentals

Reflexivity in Organisational Requirements of UK FIs

One of the ways by which IT risks may be managed in FIs is by setting up frameworks which encompass the different aspects of cybersecurity. For instance, internal control processes, security safeguards, recruitment processes, training, senior management supervision, incident monitoring and reporting, real-time behaviour systems, data loss prevention processes etc. Typically, such requirements will be reflected in the guidelines and policies of the institution and may contain certain legal and regulatory obligations which are to be followed. In the UK, for example, a number of banks adopt organisational requirements covering risk detection, certain regulatory requirements and management responsibilities.

This section analyses the 2019 Annual Reports of Barclays Bank Plc and Lloyds Banking Group which identify cyber risk as a major part of their broader risk scope. Findings from the reports are then arranged into the various stages of risk management identified in Chapter 3 to accommodate analysis. While these findings may not represent sector-wide processes, they do invariably offer insight as to the areas in which larger banks are focusing their cybersecurity resources.

The *Barclays Annual Report 2019* highlights cyber threats to its operations namely hacking to commit fraud and data manipulation, DDoS attacks, malicious emails, data breaches in payment systems.[47] The bank's 2018 report highlighted that IT operational incidents were estimated at 13% for the year 2017/18, noting a 2% decrease from the previous year 2016/17.[48] However, its 2019 report was silent on the figures for IT operational incidents in the year 2018/19. Although in its 2019 report, cyber risk was classed as an internal

[47] Barclays Plc, '2019 Annual Report' 135.
[48] Barclays Plc, '2018 Annual Report' 57 <https://home.barclays/content/dam/home-barclays/documents/investor-relations/reports-and-events/annual-reports/2018/2018-barclays-plc-annual-report.pdf> accessed 14 August 2019.

control/environment issue for which it had set up and monitored processes.[49] If robust internal control processes are implemented, cyber threats/risks and breaches will be effectively detected, assessed and prevented.[50] The report notes that it is impossible and not cost-efficient to prevent all operational risks, and as such focus would be directed at reducing risks to 'acceptable residual levels'.[51] While setting acceptable levels may favour the cost-benefit analysis, the uncertain multidimensional nature of cyber risks may render such directions impractical. To strengthen resilience and manage cyber risks, the bank adopts the following measures:

Risk Assessment Processes	A stress testing framework[52] which is useful for evaluating a firm's cyber-readiness and response.[53] The framework consists of procedures which help to detect and examine instances where the bank's corporate model may be unsustainable, for example, in the event of a cyberattack.[54] Utilises sophisticated malware detection tools to ensure data security.[55]
Risks Identified to Business Operations	Operational risks and risks to its resilience resulting from emerging technologies,[56] such as lack of adequate processes/systems, human factors or caused by fraud, data and technology risks.[57]
Risk Control Frameworks	A risk management standard set out in its Enterprise Risk Management Framework (ERMF)[58], approved by the Board on the advice of its Chief Risk Officer (CRO) who provides updates to the bank on its risk profiles.[59]

[49] Barclays Plc, '2019 Annual Report' 57 <https://home.barclays/content/dam/home-barclays/documents/investor-relations/reports-and-events/annual-reports/2019/Barclays%20PLC%20Annual%20Report%202019.pdf> accessed 6 June 2020.
[50] Z. Rezaee and others, *Business Sustainability in Asia: Compliance, Performance, and Integrated Reporting and Assurance* (Wiley 2019) 362.
[51] Barclays Plc, '2019 Annual Report' 38.
[52] ibid 71.
[53] International Monetary Fund, *United Kingdom: Financial Sector Assessment Program-Financial System Stability Assessment* (International Monetary Fund 2016) 16.
[54] Barclays Plc, '2019 Annual Report' 40.
[55] ibid 10.
[56] ibid 40.
[57] ibid 71.
[58] Containing guidance on the objectives, standards, management, identification, and reporting of risks.
[59] Barclays Plc, '2019 Annual Report' 127.

	Partnership with the Cyber Defence Alliance (CDA)[60], a public-private organisation which promotes cyber defence capabilities across banks and the sharing of information/intelligence in the financial services sector. The implementation of the GDPR to enhance the protection of identifiable, financial, intellectual property and customer data from risks to its availability, integrity and confidentiality.[61]
Risk Review	An intelligence-centred security process for examining external situations for evolving cyberthreats and the implementation of cyberthreat scenarios to evaluate its security frameworks and operational effects and conducts hacking simulations to test system preparedness.[62] Considerations on the impact of third-party relationships where there are resilience and recovery incapability in technological processes[63] which may pose reputational, compliance and even legal risks.[64]

Table 4-1 *Risk management frameworks adopted by Barclays Bank Plc*

Cybersecurity and data security are indicated as key factors for maintaining customer confidence in the Lloyds Bank Annual Report.[65] The bank faces a number of internal challenges including developing effective and resilient IT response systems.[66] Implementing resilient IT response systems and mitigating evolving cyber threats an integral part of risk assessment and management processes.[67] To strengthen its cyber defences resilience and prevent the risk of fraud, the bank adopts the following measures:

Risk Assessment Processes	Implementation of security measures such as disruptive technologies, DDoS capabilities, access and network security controls to prevent threats to the availability confidentiality and integrity of data and systems.

[60] ibid 337.
[61] Lloyds Banking Group, '2019 Annual Report' 135 <https://www.lloydsbankinggroup.com/globalassets/documents/investors/2019/2019_lbg_annual_report_v3.pdf > accessed 6 June 2020.
[62] Barclays Plc, '2019 Annual Report' 202.
[63] ibid 134.
[64] D. Barrett, M.M. Weiss and K. Hausman, *CompTIA Security+ SYO-401 Exam Cram: Comp Secu SY04 Auth ePub _4* (Pearson Education 2015) 106.
[65] Lloyds Banking Group, '2019 Annual Report' 12.
[66] ibid 14.
[67] Y.Y. Haimes and A.P. Sage, *Risk Modeling, Assessment, and Management* (Wiley 2015), *Risk Modeling, Assessment, and Management* (Wiley 2015) 59.

	Internal controls and third-party/supplier system's testing[68]
Risks Identified to Business Operations	Cyber-related risks such as data and operational resilience risks previously highlighted in its 2018 report as existing and emerging risks.[69] This have now been escalated in its 2019 report as principal risks to its business e.g., a failure to effectively supervise its outsourcing arrangements, business continuity risks and poor risk management systems.[70]
Risk Control Frameworks	Incorporating a cyber control framework compatible with industry credited cybersecurity standards i.e., the National Institute of Standards and Technology (NIST).[71] An outsourcing policy to ensure that third-party arrangements adhere to specific due diligence, risk assessment and continuing assurance policies.[72] Collaboration with the government and relevant industry partners to ensure security of customer's data and finances through the banking protocol[73], membership of the Cyber Collaboration Centre, implementing regulations of the GDPR and partnership with the CDA.[74] Implementing an ERMF approved by the Board and senior management on the advice of the CRO, and risk governance through the delegation of authority.[75]
Risk Review	Key Risk Committees are responsible for cyber risk governance and conduct a quarterly review of all cyber risks.[76] Stress testing is carried out to evaluate the effect of potential risk scenarios with results used to inform strategic responses.[77]

[68] Lloyds Banking Group, '2019 Annual Report' 92.
[69] Lloyds Banking Group, '2018 Annual Report' (19 February 2019) 74 <https://www.lloydsbankinggroup.com/globalassets/documents/investors/2018/2018_lbg_annual_report_v2.pdf > accessed 14 August 2019.
[70] Lloyds Banking Group, '2019 Annual Report' 42.
[71] A US Cybersecurity Framework which sets out guidance for best cyber security practices which organisations and businesses may adopt. It identifies five relevant cyber security risk management functions i.e., identification, protection, detection, response, and recovery.
[72] Lloyds Banking Group, '2019 Annual Report' 140.
[73] The banking protocol is an innovative rapid response scheme by which bank staff may send signals to police and trading standards on suspected frauds occurring.
[74] Lloyds Banking Group, '2019 Annual Report' 26.
[75] ibid 40.
[76] ibid 133.
[77] ibid 131.

	Enhanced corporate and personnel engagement through education and awareness, an information management model[78] and phishing exercises.

Table 4-2 *Risk management frameworks adopted by Lloyds Banking Group*

Findings from both reports show the use of both reactive and proactive cybersecurity processes to assess and identify security risks, define regulatory and organisational requirements to be implemented for mitigating identified risks and then, conducting analysis of its processes to measure system responses to threat scenarios for the purpose of decision making. The reports show an understanding of availability, confidentiality, integrity and outsourcing risks identified in Chapter 3.

Both reports also suggest that the Board and Chief Risk Advisor play a crucial role in the policy decision making of an organisation's cyber risk profile, a function that needs to be considered in many regulatory systems. Findings also show the collaboration/coordination with various industry partners on different programmes, a step which is crucial to improving information sharing and facilitating regulation. It also places FIs in the right angle for learning from and receiving guidance and support through the information and capabilities resulting from these partnerships.

In summary, both reports reflect the positive attitudes of institutions towards strengthening operational resilience, but also suggest the need for banks to focus on developing systems with effective internal control processes.

4.5 Reflexivity in Regulation and Supervision

In the UK, the FCA employs a risk-based and proportionate approach to regulation, in which it prioritises its resources to businesses which pose greater risk to its statutory objectives. It uses knowledge from established evidence to make policy decisions to influence the behaviour of FIs.[79] The FCA prioritises and manages current cyber risks through a

[78] Information management models consists of standards for generating, obtaining, handling, storing, retrieving, transmitting, and erasing data/information in Eric Cole, *Network security bible*, vol 768 (John Wiley & Sons 2011) 43.

[79] Financial Conduct Authority, 'The FCA's approach to advancing its objectives' (July 2013) 8 <https://www.fca.org.uk/publication/corporate/fca-approach-advancing-objectives-july-2013.pdf> accessed 4 August 2019.

collaborative supervisory operation with other authorities, in FIs at risk, and keeps smaller FIs informed on cyberattacks, advances specialist capabilities and addresses major regulatory international concerns.[80]

The PRA's Rulebook sets out comprehensive requirements which by their 'influencing' effect, may reflexively enhance the operational resilience of a FI by choosing which rules to focus on in addressing risks. Meanwhile, the FPC through the stability report raises awareness of operational cyber incidents and ways by which regulated entities may develop capabilities[81] and the importance of operational resilience for individual firms and consumer protection.[82]

In this section, we discuss regulatory reflexivity under a number of headings: receiving cyber incident communications, conducting simulation tests and exercises, outsourcing arrangements and information disclosure and reporting. ***Table 4-3*** below shows a regulation of risks involving a multi-actor network, prescribed guidelines which allow for flexibility in their implementation which are key features of a reflexive system. For requirements which must be expressly followed, these reflect features of command-and control systems, where regulators may issue sanctions for a breach, as identified in this chapter.

Regulator	Requirements
FCA	• Principle 11 and SUP 15.3 of the FCA Handbook: notifications and communications on cyber incidents from FIs to the FCA or appropriate regulator[83] *any* issues in which the regulator would reasonably expect to be notified.[84] • implementation of the CBEST framework, an intelligence-driven framework used in assessing and testing a firm's IT or cyber resilience

[80] Financial Conduct Authority, 'Business Plan 2019/2020' 8.
[81] Bank of England, 'Financial Stability Report (Issue No. 41)' (June 2018) 40 <https://www.bankofengland.co.uk/-/media/boe/files/financial-stability-report/2018/june-2018.pdf> accessed 19 August 2019.
[82] ibid 41.
[83] Appropriate regulators may include regulators in recognised jurisdiction with respect to electronic money, payment services and other regulated activities.
[84] Financial Conduct Authority, 'Principles for Businesses' (August 2019) Schedule 2.2G <https://www.handbook.fca.org.uk/handbook/PRIN.pdf> accessed 4 August 2019.

	• *FG16/5 Guidance for Firms Outsourcing to the 'Cloud' and other Third-party IT Services* which sets out requirements for firms to consider in their outsourcing arrangements.[85] • SYSC 4.1.1R(1)1: implement internal controls, security programmes for information processing systems. • Principle 3: implement adequate risk management systems and apply reasonable care in the control and organisations of operations.
PRA	• carrying out operations with due skill, care and diligence (Rule 2) and operating in a prudent manner (Rule 3); and engaging with regulators in an open way, including making appropriate disclosures of relevant matters (Rule 8).[86] • general organisational requirements for internal control mechanisms, risk management, disclosure and reporting; implementing frameworks for ensuring the security, integrity and confidentiality of information; and contingency and business continuity strategies.[87]
FPC	• expressly stated minimum requirements for firms' resilience • continuous test of resilience by firms and supervisors • identifying firms which fall outside the financial regulatory borderline • clear and tested response metrics in the event of a cyber incident.[88]

Table 4-3 *Regulatory Guidelines Associated with Reflexivity in the UK*

Conducting Simulation Tests and Exercises

In carrying out their cybersecurity functions, regulators may conduct tests or exercises in the firms it regulates to assess the effectiveness of their cybersecurity systems and response plans as well as enhance their preparedness in response to cyber incidents.

[85] Financial Conduct Authority, 'FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services' (July 2018) <https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf> accessed 4 August 2019.
[86] Bank of England, 'Prudential Regulation Authority: Fundamental Rules and Principles for Businesses' <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/new-bank/fundamentalruleprinciples> accessed 9 August 2019.
[87] Bank of England, 'PRA Rulebook' Rule 2 <http://www.prarulebook.co.uk/rulebook/Content/Part/214136/15-08-2019> accessed 10 August 2019.
[88] Bank of England, 'Financial Stability Report (Issue No. 41) PART B - Banking Sector Resilience' (June 2017) 27.

In the UK, there is a collaborative work between the FCA, other regulators, security experts and the Council for Registered Ethical Security Testers (CREST) in developing the CBEST framework. The CBEST is used for the purpose of increasing the understanding and awareness of firms on the forms of cyberattacks which affect the stability of UK financial markets as well as the degree of vulnerability of the market to those attacks.[89] The framework consists of four phases namely the initiation, threat intelligence, penetration testing and closure phase,[90] and shapes the context in which reflexive learning may be achieved through design, development, implementation and review. In particular, results from the penetration testing inform remedial processes.[91] Indeed, the framework encourages FIs to examine the risks they are being faced with, then develop the procedures and appropriate capabilities required to manage them.

Outsourcing Arrangements

Third-party outsourcing arrangements are major source of data breaches and may be associated with quality risks, security risks, reputational risks, and associated regulatory costs for non-compliance. In response to this issue, the FCA issued the *FG16/5 Guidance for Firms Outsourcing to the 'Cloud' and other Third-party IT Services* which set out requirements for firms to consider in ensuring security in their outsourcing arrangements. As part of its requirements, FIs are to comply with the provisions of privacy, data protection and network security legislation which will be considered later in this chapter.[92]

Some risk management requirements in the guidance provide interesting examples of what standards FIs may follow as a means of ensuring reflexive governance of its outsourcing arrangements. These include conducting and recording risk assessments; determining mitigation plans; specifying existing sector-wide good practices; and setting requirements for managing cyber risks, data and information security systems.[93] Specifically, it gives proactive guidance in considering measures which may be put in place should

[89] Bank of England, 'CBEST Intelligence-Led Testing: An Introduction to Cyber Threat Modelling' *Version 2.0* (2016) 19.
[90] ibid figure 2.3.
[91] ibid para 6.5.
[92] Financial Conduct Authority, 'FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services' (July 2018).
[93] ibid 6 - 7.

outsourcing arrangements fail and recommends that concentration risk be supervised. This is probably owing to risks that may arise where a service provider undertaking multiple outsourcing arrangements becomes a victim of a cyberattack. Hence, confirming the argument in Chapter 3 that reflexive cybersecurity approaches require a combination of measures that proactively and reactively mitigate the risk of a cyberattack.

Information Disclosure and Reporting

Financial disclosure is important because disclosure not only provides an understanding of the cyber risk landscape, but also enables the development of effective response techniques through information sharing, and regulation helps to ensure that disclosure is done in public interest. However, there is often low disclosure by FIs due to fear of reputational damage, financial and market losses.[94] Particularly, due to concerns that disclosures will expose weaknesses in their cybersecurity systems. These concerns have been highlighted by Barclays Plc as increase in fraud losses, customer detriment, the inability to carry out necessary economic activities, legal liability and financial penalty or regulatory censures.[95]

In the UK, the FCA is authorised to receive cyber incident and data breach reporting obligations contained in regulatory guidance, with a similar provision contained in legislation. The notification requirement in Principle 11 and SUP 15.3 of the FCA Handbook extends to the reporting of material cyber incidents. As noted under the FCAs publication 'Good Cybersecurity - the foundations', a cyber incident may be material and should be reported if it "brings about a significant loss of data, or the availability or control of IT systems or infrastructure, affects a significant amount of consumers, results in unauthorised access to and/or causes malware to be present on information and communication systems".[96] Despite this guidance, the criteria for defining what amounts to a 'material' breach may be subject to different interpretations, an incoherent understanding of the nature and implication of the breach, and thus, fragment regulatory efforts.

[94] J.L. Richet, *Cybersecurity Policies and Strategies for Cyberwarfare Prevention* (IGI Global 2015) 169.
[95] Barclays PLC, 'Return to Stability - Annual Report 2015' (2015) 122 <https://www.home.barclays/content/dam/barclayspublic/docs/InvestorRelations/AnnualReports/AR2015/Barclays_PLC_Annual_Report_%202015.pdf> accessed 13 April 2018.
[96] Financial Conduct Authority, 'Good cybersecurity - the foundations' (2017).

The FCA also publishes Discussion Papers jointly with other regulators on developing a sound cybersecurity framework e.g., Paper on building operational resilience of financial services firms in which it sets outs risks presented by cyberattacks and other operational IT-related incidents.[97] Such publications aid reflexive learning, in that, FIs may learn how to adapt their systems to better deal with identified risks.

In July 2018, the FCA jointly published a Discussion Paper jointly with the PRA and FPC regarding building up the operational resilience of financial services firms in which it sets outs risks presented by cyberattacks and other operational IT-related incidents and emphasises the need to be wholly resilient due to the sector's growing reliance on, and interconnection *via* data and technology. In the paper, the effective resilience required of firms were viewed broadly as:[98] the prevention of material cyber incidents from taking place; business continuity during the incident; mitigating the rise in fraud levels in the course of the incident; ensuring that activities are up and running once the incident has ended; and improving understanding from incidents, so as to prevent a reoccurrence. The guidance shows that FIs are expected to implement mainly proactive resilience standards, however, because of the possibility that an attack may occur before it is being detected, they also favour reactive standards to enhance resilience.

4.6 The 'Regulatory Co-Existence' Hypothesis

The co-existence hypothesis is based on the notion discussed in Chapter 3, that regulation of FIs is not constrained to self-regulation, but regulation against a backdrop of state regulation. Our starting point for validating this hypothesis is by exploring examples of how the government through relevant regulatory authorities, enforces applicable laws and regulations through the issuing of penalties for cybersecurity breaches and misconduct.

[97] Bank of England, 'Discussion Paper 01/18: Building the UK financial sector's operational resilience' (July 2018) 13 <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf?la=en&hash=4238F3B14D839EBE6BEFBD6B5E5634FB95197D8A> accessed 8 August 2019.
[98] ibid.

Then, we will examine instances where responses to the risk landscape requires a partnership with public actors and gives rise to intervention for the purpose of criminal law enforcement.

Civil Fines and Penalties: FCA's Sanctioning Regime

In the past, the FCA's predecessor, the FSA has shown its readiness to impose fines on banks which fail to comply with its Principles. For instance, in July 2009, it fined HSBC Life UK Limited and others,[99] a total of £3,175,000 for data security failures. The firms were found to be in breach of Principle 3[100] of the FSA's principles for businesses relating to IT system and control failures regarding the security of customers data. In its notice, the FSA noted that these firms had not put in place adequate measures for protecting customers' personal data against risks like data loss, financial loss and identity theft. Other failings included the lack of effective frameworks for timely reporting of data losses and risk assessment, and outdated training for staff on data security measures. By so doing, they were liable for the requirements and amount imposed upon them by the FSA in accordance with Section 206 of the FSMA 2000. Similarly, Zurich Insurance (UK) Plc, a firm from the European Economic Area (EEA), was fined £2,275,000, where there had been a breach of Principle 3 and SYSC rules 3.1.1R and 3.2.6R relating to the security of its customer data in relation to data security of customers information connected with data outsourcing arrangements to third party suppliers.[101]

The FCA, has in recent times taken a similar approach to the FSA in exercising its enforcement powers on IT operational incidents. This is represented in the table below.

Cyber Incident Examples	Applicable Laws and Regulations	Regulatory Costs and Penalties
• Failure to respond appropriately to disruptions,	Principles 2 requiring the exercise of due skill, diligence and care in operations and	Joint fine with the PRA of £1.89 million

[99] Financial Services Authority, 'Final Notice: HSBC Life (UK) Limited' (17 July 2009) <http://www.fsa.gov.uk/pubs/final/hsbc_inuk0907.pdf> accessed 21 June 2018.
[100] Financial Conduct Authority, 'PRIN2.1.1: The Principles' (3 January 2018) <https://www.handbook.fca.org.uk/handbook/PRIN/2/?view=chapter> accessed 21 June 2018.
[101] Financial Services Authority, 'Final Notice: Zurich Insurance (UK) Plc' (19 August 2010) <http://www.fsa.gov.uk/pubs/final/zurich_plc.pdf> accessed 21 June 2018.

	and IT failings in its outsourcing systems Raphaels Bank 2019[102]	Principle 3, as well as SYSC 8 on general outsourcing requirements	
•	IT and Technology failures in Tesco Bank 2016[103]	Principle 2 FCA Handbook	Fine of £16.4 million
•	Standard Chartered Bank failings in oversight of its correspondent banking, AML controls and shortcomings in online banking systems.[104]	Regulations 7(1) to (3), 8(1) and (3), and 14(4) of the Money Laundering Regulations 2007	Fine of £102.2 million
•	RBS Group IT systems failure and disruption 2014.[105]	Principle 3 FCA Handbook requiring adequate risk management systems and controls.	Fine of £42 million

Table 4-4 *Examples of UK FCA's Cybersecurity Sanctions*

The use of sanctions for rule enforcement, as can be seen in these cases may serve as a caution to FIs where they fail to comply with requirements. The question, however, is how well the sanctions may help to achieve the objective of reflexivity. Some of the ways by which sanctions may encourage learning is the carrot approach where regulators provide incentives to FIs for taking steps to contain an incident and prevent further losses or the stick approach where uncooperative FIs face the risk of further punishment. For instance, in the Tesco case, the FCA offered a 30% discount on its fines because the bank cooperated with investigation, initiated an assessment of its systems to ensure no customer data was lost,

[102] Financial Conduct Authority, 'Final Notice: R. Raphaels & Sons Plc' (29 May 2019) <https://www.fca.org.uk/publication/final-notices/r-raphael-sons-plc-final-notice-2019.pdf> accessed 4 August 2019.
[103] Financial Conduct Authority, 'Final Notice: Tesco Personal Finance Plc'.
[104] Financial Conduct Authority, 'Decision Notice: Standard Chartered Bank 2019' (5 February 2019) <https://www.fca.org.uk/publication/decision-notices/standard-chartered-bank-2019.pdf> accessed 4 August 2019.
[105] Financial Conduct Authority, 'Final Notice: Royal Bank of Scotland Plc, National Westminster Bank Plc and Ulster Bank Ltd' (19 November 2014) <https://www.fca.org.uk/publication/final-notices/rbs-natwest-ulster-final-notice.pdf> accessed 4 August 2019.

reviewed its payment control systems, offered customers redress and communicated its responses to the regulators.[106]

It is important to note that, in deciding the appropriate level of penalty, the FCA is guided by three principles.[107] First, Disgorgement i.e., an institution or person should not profit from the breach, supporting the Kriesberg Rational Actor Model in Chapter 3 which suggests that one of the ways to criminalise wrongdoings, is to consider the background rational values. Second, Discipline i.e., an institution or person ought to be reprimanded for misconduct. Thirdly, Deterrence i.e., any fees imposed must achieve a preventive effect in the institution or person where the breach was committed and in other institutions to build up risk management systems, so as not to suffer a similar fate. The total penalty imposed on an institution or person involved in an enforcement action may be made up of the disgorgement of the advantage gained and reflective of the seriousness of the breach.[108] Similar to the approach and avoidance perspectives to developing systems of self-regulation in human psychology, indicators of rewards and punishments are believed to influence goal-oriented behaviours.[109] Thus, suggesting that the FCA's approach may encourage positive conduct in FIs and subsequently, enhance accountability.

Prescribing punishments reflective of the seriousness of the offence is found in the long-standing principle of proportionality under criminal law which assumes beliefs of justice and fairness. Indeed, it has been observed that great considerations of this principle in sanctioning, satisfies the just deserts rationale.[110] Recent considerations have revealed a weak link in this approach as there is not a universal measurement or consensus for determining what makes a crime more or less serious than the other.[111] As Tonry confirms, there are difficulties which arise from possible differences in how an offender and victim conceive a crime (i.e. based on awareness and impact, respectively), and how a crime may result in varying harmful consequences. Such difficulties of associating punishments with varying

[106] Financial Conduct Authority, 'Final Notice: Tesco Personal Finance Plc' 24 - 25.
[107] FCA Handbook, DEPP 6.5.2.
[108] FCA Handbook, DEPP 6.5.3.
[109] Daniel Brass and others, *Contemporary perspectives on organizational social networks* (Emerald Group Publishing 2014) 231.
[110] Andrew Von Hirsch, 'Proportionality in the Philosophy of Punishment' (1992) 16 Crime and Justice 55, 56.
[111] Michael Tonry, 'Proportionality Theory in Punishment Philosophy: Fated for the Dustbin of Otiosity?' (2019) *Of One-eyed and Toothless Miscreants: Making the Punishment Fit the Crime* 13.

degrees of harmfulness of a crime have been examined in earlier literature. Specifically, Von Hirsch elucidates the approach of Cardinal and Ordinal Proportionality involving set primary scales of penalties like minimum and maximum sentences, that a system can impose for specific crimes based on its seriousness, and involving set punishments reflective of the gravity of the crime on a corresponding level of severity with punishment of other crimes (recognising, mitigating or aggravating factors), respectively.[112] Given this, it appears that combined approaches have been followed where certain cybersecurity regulations which have set penalty scales have been implemented taking into consideration mitigating factors such as regulatory cooperation and prompt remedial actions, ultimately resulting in a reduction of fines.

Still, for cyber incidents, it would be impractical to limit the deciding factor to losses suffered or harm caused without considering other values like the time frame of exposure, the system's state of readiness, data breach notification etc. To this effect, the UK's Network and Information Systems Regulation 2018 discussed later in the chapter, serves as an evidence of proportionality standards in cybersecurity regulation, with provisions requiring proportionality and appropriateness of penalties to IT failures and setting factors for determining cybersecurity incidents with a material effect. Such factors include duration of incident, persons affected by the incident and the geographic reach of the incident.

4.7 Criminal Justice Responses Applicable to UK FIs Under Legislation

There are several cybersecurity requirements contained in industry, domestic and international legislation, regulations and standards that significantly influence and shape the sector's cyber risk management processes.

Industry Cybersecurity Standards

ISO/IEC 27001 and 27002:2013

The ISO 27001 is an international standard applied by many FIs globally as it sets outs requirements which institutions may apply to manage their information security systems. The

[112] Andrew von Hirsch, 'Proportionality in the philosophy of punishment: From "why punish?" to "how much?"' (1990) 1 Criminal Law Forum 259, 282.

ISO 27001 and 27002 standards originate from the works of the UK British Standards Institution and Department for Trade and Industry.[113] In the UK financial services sector, the standard is recommended as a benchmark for developing good practices in institutions.[114]

The ISO 27001 and 27002 provides information security management systems framework which may be adopted by institutions or considered when implementing best practices. These cover codes of practice for information security controls, security techniques, compliance, cryptographic controls, information security incident management, asset management, amongst others.[115] In particular, the ISO 27001 specifies risk assessment criteria which institutions must take into account such as identifying confidentiality, availability and integrity risks to its information assets and systems, and requires that processes be put in place for risk acceptance levels, albeit failing to provide clarity as to how these levels may be defined. Nevertheless, effective implementation of the framework is believed to facilitate compliance with other cybersecurity regulations due to the comparability of its requirements with operational frameworks.[116]

International Response to Cybercrime

Budapest Convention on Cybercrime

As far as the UK is concerned, it signed the Convention in November 2001, ratified it in May 2011 and it came into force in September 2011. The delay in the ratification was believed to be largely based on the fact that UK law was incompatible with the provisions of the Convention.[117] The Budapest Convention attaches great importance to cooperation and unity between COE's member states towards preventing cybercrime as the term "cooperation" appeared eight times in the treaty document.[118] This has, in the past, been described by David

[113] J. Hamid, M. Gianluigi and W.D. Lilburn, *Handbook Of Electronic Security And Digital Forensics* (World Scientific Publishing Company 2010) 226.
[114] Financial Conduct Authority 'Cybersecurity - industry insights' (March 2019) para 2.2 <https://www.fca.org.uk/publication/research/cyber-security-industry-insights.pdf> accessed 10 August 2019.
[115] U. Nayak and U.H. Rao, *The InfoSec Handbook: An Introduction to Information Security* (Apress 2014) 38.
[116] Stefanos Gritzalis and others, *Trust, Privacy and Security in Digital Business* (Lecture Notes in Computer Science 2019) 100.
[117] S. van der Hof and others, *Sweetie 2.0: Using Artificial Intelligence to Fight Webcam Child Sex Tourism* (T.M.C. Asser Press 2019) 295.
[118] Council of Europe, 'Cybercrime Convention CETS 185' (23 November 2001) 2 - 3 <https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf> accessed 9 August 2019.

Cameron, the former UK Prime Minister as "[a way of] … ensuring a more cohesive EU approach to cyber issues".[119] However, the likelihood of a more unified approach post-Brexit, after the UK leaves the EU, remains questionable.

The Convention requires that its signatories adopt a number of measures including enforcement of 'effective, proportionate and dissuasive' sanctions,[120] real-time collection of computer data,[121] and cooperation among parties to the convention.[122]

Domestic Legislation/Regulation relating to Cybersecurity for FIs

The Table below sets forth the laws which provide cybersecurity requirements for UK FIs to follow.

Payment Services Regulations (PSRs) 2017	The Regulation sets out requirements covering the establishment of appropriate security control frameworks taking into account risk detection and incident response towards the management of cybersecurity risks. In addition, the Regulation contains incident reporting requirements similar to that of the FCAs Principle 11.
Data Protection Act (DPA) 2018	The legislation makes provision for a variety of data access and control offences and requirements including: the requirement for data controllers (in this case, FIs) to set up appropriate technical and organisational measures in place for the security and processing of personal data;[123] and mandatory reporting of personal data breach to the Information Commissioner[124] and customers.[125]
NIS Regulations 2018	The Regulations sets out comprehensive requirements aimed at enhancing the security of network and information systems. For instance, it places obligations on Operators of Essential Services (OES) to adopt appropriate

[119] G.B.P.H.C.E.S. Committee and W. Cash, *Fortieth report of session 2012-13: documents considered by the Committee on 24 April 2013, including the following recommendations for debate, adjustment of direct farm payments for 2013; enhanced cooperation and financial transaction tax; 2013 General Budget, report, together with formal minutes* (Stationery Office 2013) para 4.19.
[120] Council of Europe Convention on Cybercrime, Article 13.
[121] Council of Europe Convention on Cybercrime, Article 20.
[122] Council of Europe Convention on Cybercrime, Article 23.
[123] Data Protection Act 2018, Section 56.
[124] Data Protection Act 2018, Section 67.
[125] Data Protection Act 2018, Section 68.

	security measures in managing risks posed to its network and information systems[126] and in the notification of cybersecurity incidents.[127]

Table 4-5 *UK Laws Specifying Cybersecurity Best Practices*

PSRs 2017

The Regulation implements the revised Payment Services Directive (PSD2)[128] providing regulatory guidance for payments services and electronic money systems. Regulation 98 of the PSRs 2017 is the regulation on risk management which provides that:

"Each payment service provider (PSP) must establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services it provides [and]. . . establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents".[129]

Under the Regulation, a PSP must provide the FCA with an up-to-date and detailed review of risks to its IT security and operations and the procedures and controls implemented in response to such risks. In effect, PSPs are obliged to notify the FCA of any significant operational or security incident and inform its payment service users of such an incident, where the incident has or may have affected the financial interests/transactions of such users to enable them take relevant mitigative measures.[130]

DPA 2018

The Act complements the EU's General Data Protection Regulation (GDPR) underpinning the regulation and protection of data and replaces the DPA 1998. The GDPR sets standards for businesses within the EU and global organisations with businesses located in the EU. It identifies areas to be taken into account by organisations that are data controllers and processors, to prevent the threat of a data loss or breach which can be devised or exploited by

[126] Network and Information Systems Regulations 2018, Article 10.
[127] Network and Information Systems Regulations 2018, Article 11.
[128] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, and 2013/36/EU.
[129] Payment Services Regulations 2017, Regulations 98(1).
[130] Payment Services Regulations 2017, Regulations 99.

cybercriminals. FIs fall within this scope as they control and process various forms of data for different purposes including accounting, credit checks, customer registration and verification etc. Some of the key issues provided for in the DPA, in accordance with the GDPR include designating a data protection officer in an organisation responsible for addressing issues relating to the protection of personal data;[131] and the Commissioner's powers to impose significantly high administrative fines,[132] subject to a penalty notice.[133]

The Act contains obligations which have direct risk management implications for institutions like FIs who carry out activities involving the control and processing of personal data. Section 66 of the DPA 2018 provides that:

> Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data.

From this obligation, there appears to be an implication of an ongoing process, one which requires that the security measures be tailored on the basis of a constant assessment of the risks. Specifically, the phrase 'risks arising from the processing of personal data', indicates awareness of an evolving nature of risks, and may include security considerations for risks that occur, or risks predicted to occur in the course of operations. Given that, the term 'appropriate' would then imply that technical and organisational measures adopted must be suitable as well as adequate and may involve reactive and proactive measures that are appropriate in the way which they ensure resilient recovery in the event of a cyberattack or mitigate against cyber vulnerabilities. An obligation such as this which allows for learning and remodification of processes provides an example of a reflexive approach to cybersecurity regulation.

Relevant authorities may impose fines on FIs for breach of data protection duties provided for under the GDPR, subject to certain requirements. Without following the provisions of the GDPR, it is possible for firms to face serious consequences for non-compliance. Under the law, firms may face huge financial penalties of up to €20million or

[131] Data Protection Act 2018, Section 69 – 71.
[132] Data Protection Act 2018, Section 58(2)(i) and Article 83 of the GDPR.
[133] Data Protection Act 2018, Section 155.

four percent of their annual turnover for serious breaches (whichever is higher) and up to €10million or two percent of their annual turnover for less serious breaches (whichever is higher).[134] From this, it would seem to me that the law seeks to encourage self-regulation through provisions which allow firms to implement measures proportionate to the risk levels they face, while it seeks to deter non-compliant behaviours using fines and penalties - measures typical to a 'command and control' regime. This distinction has important implications for future cybersecurity regulation.

Section 68 of the DPA 2018 provides for the reporting of a breach and notes that:

> [T]he controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of individuals.

This provision is quite explicit in the way that it classifies risk (to the rights and freedoms of natural persons) and high risk (to the rights and freedoms of the natural person). It indicates different levels of risks and recognises instances where a breach is material even when it affects only a small number of customers. In light of this, the Act makes provision for conducting data protection impact assessments where a form of processing has the potential to pose high risk to the rights and freedoms of persons.[135] Such forms of processing may involve third parties who may take a significant amount of control over certain data or IT operations of an organisation.[136] Where a bank employs the services of an IT company to process data on its behalf, the provisions of the DPA 2018 seeks to ensure that the outsourcing provider has regard for the protection of data subjects' rights and freedoms in whatever processing measure it applies by requiring the implementation of "security measures appropriate to the risks arising from the processing of personal data".[137] For instance, in the Raphaels investigation, where IT failings in its outsourcing arrangements resulted in service disruption for about 5,356 of its customers, over a duration of 8 hours, it was found that the firm failed to monitor, instruct and oversee its outsourcing arrangement and related business continuity processes.[138]

---

[134] General Data Protection Regulation, Article 83 (4) - (6), Data Protection Act 2018, Section 157.
[135] Data Protection Act 2018, Section 64.
[136] H. Bidgoli, *Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations* (Wiley 2006) 131.
[137] Data Protection Act 2018, Section 107.
[138] Financial Conduct Authority, 'Final Notice: R. Raphaels & Sons Plc' para 2.8.

Such failings will amount to an infringement of the Act which would have potentially cost Raphaels and its sub-contracted processors, a large percentage of their annual revenues as liability applies not only to organisations in control of data, but also third party organisations to whom access to data has been granted for the purpose of processing.

Upon closer look at the FCA's decision in the Tesco Bank case, the scope of application of the Act in the financial services sector appears uncertain. In fact, the decision raises important questions with regards to cybersecurity regulation. In its final notice, the FCA notes the exploitation of an algorithm in producing the bank's customers' debit card details but claims that there was no loss or theft of personal data.[139] This is highly arguable. With the wide scope of the DPA 2018, there is a risk that the bank's failings would have amounted to a breach under Section 66 of the DPA 2018 and Section 57 of the DPA 2018 relating to the implementation of security measures which are designed to ensure data protection and safeguards of processing. While the fines imposed in this case appears to be almost within the range of the higher maximum penalty imposed under the Act, it does raises questions about how the FCA will deal with similar future cases and whether it would consider higher fines.

Regardless of the approach being followed, it is important to note that the personal data protection breaches are been perpetrated in such a way that involves breaches to the security of an organisation's network and information systems. This, in effect, falls under the scope of the NIS Regulations 2018 and may suggest additional liabilities for Tesco Bank. To fully appreciate implications of cybersecurity regulations for FIs, the NIS Regulations 2018 and its relation to the DPA 2018 are discussed below.

NIS Regulations 2018

The Regulations implement the NIS Directive[140] which aims to 'attain a high common level of network and information systems security within the EU'[141]. The Directive requires the designation of a competent authority to oversee the implementation of the Directive[142] and a

[139] Financial Conduct Authority, 'Final Notice: Tesco Personal Finance Plc' para 2.1.
[140] Directive 2016/1148 of the European Parliament.
[141] Network and Information Systems Directive, Article 1.
[142] Network and Information Systems Directive, Article 8.

Computer Security Incident Response Team (CSIRT). The GCHQ is the CSIRT designated for digital services and relevant sectors[143], satisfying a requirement set by the NIS Directive.[144] The directive further places reporting and risk management requirements on the operators of 'essential services' such as those in 'banking'.[145]

The inadequacy of cybersecurity safeguards against cyber incidents and risks across the EU is recognised in the Directive.[146] On risk management standards, Recital 44 of the NIS Directive provides that:

> A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed through appropriate regulatory requirements and voluntary industry practices.

The implementation of the NIS Regulations 2018 is aimed at introducing legal frameworks to:

> Ensure that essential services and selected DSPs within the UK implement adequate procedures to enhance their network and information systems security, with a particular focus on those services which if disrupted, could potentially cause significant damage to the UK's economy, society and individuals' welfare; and to ensure serious incidents are promptly reported to the competent authorities.[147]

The OES in the UK are identified in paragraphs 1 to 9 of Schedule 2 and designated competent authorities for OES are identified in Column 3 of the table under Schedule 1 of the Regulations. OES identified in the Regulations include the energy, transport, health, drinking water and digital infrastructure sectors. From the guidance provided under Annex II of the NIS Directive, it appears obvious that the banking and financial market infrastructures sectors should have been included in this list. Yet, surprisingly enough, as at the time of writing, there has been no step taken towards inclusion of the sectors under the Regulations.

[143] Network and Information Systems Regulations 2018, Regulation 5.
[144] Network and Information Systems Directive, Article 9.
[145] Network and Information Systems Directive, Article 14.
[146] Network and Information Systems Directive, Recital 5.
[147] Explanatory Memorandum to the Network and Information Systems Regulations 2018 No. 506, para 2.1.

Prior to its implementation of the NIS Directives, the UK Government collected a total of 358 responses to the consultation paper on the Security of Network and Information Systems. Majority of those who replied were of the opinion that the proposals excluded a few sectors/service providers which they believed should have been covered, including the financial sector.[148] In the analysis of responses to the public consultation, it was reported that consultees regarded penalty structures under the GDPR and NIS rules as having the tendency to jeopardize the financial stability of businesses and result in conflicts with certain financial resilience regulatory objectives[149], such as those pursued by the FCA, PRA and BoE. Meanwhile, smaller sections of consultees found the penalties insufficient and believed additional criminal sanctions should be included.[150] Although, the paper does not specify the types of criminal sanctions being considered, questions arise as to whether these may include the criminal liability of designated cybersecurity executives discussed in Chapter 3.

There were also concerns over double jeopardy, where OES and DSPs risk liabilities under both the GDPR and NIS. While acknowledging validity of the concerns, the Government observes that situations may arise requiring distinct penalties under the two regimes for a single incident where penalties involve specific parts of the offence and different impacts.[151]

The European Commission in a 2019 Report assessing the consistency in the approach taken to identify operators of essential services, expressed its dissatisfaction in the approach followed by some of its members states (which the UK was a member) in applying the *lex specialis* principle. The principle enshrined in Article 1(7) and in accordance with Recital 9 of the NIS Directive, allows for an exemption of a sector if there is an existing EU

[148] Department for Digital, Culture, Media and Sport, 'Security of Network and Information Systems Public Consultation' (August 2017) 6 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf> accessed 12 December 2020.
[149] Department for Digital, Culture, Media and Sport, 'Analysis of responses to public consultation: Security of Network and Information Systems' (January 2018) 25 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677066/NIS_Consultation_Response_-_Analysis_of_Responses.pdf> accessed 12 December 2020.
[150] ibid 26.
[151] Department for Digital, Culture, Media and Sport, 'Security of Network and Information Systems: Government Response to Public Consultation' (January 2018) 16 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf> accessed 13 December 2020.

legislation providing at the very least, requirements identical to those of the Directive, and imposing notification and security obligations on the operators of essential services. On this basis, the UK argues that the sector is already regulated by other specific EU Directives.[152] Perhaps the GDPR (DPA 2018), arguably constitutes an example of such legislation as it is mentioned severally across the reports of financial services regulators. While the DPA 2018 may provide efficient cybersecurity standards, it is believed that these are not sufficient, particularly in the financial services sector.

In the report, the Commission notes that although many EU member states included the banking and financial markets sectors as operators of essential services, some others have declined to do so, asserting that this falls under *leges specialis*.[153] Further, the Commission notes its commencement of thorough reviews through state visits in evaluating the transposition and implementation of the Directive across the EU, as well as the *lex specialis* requirements. However, it appears that this objective will not be realised in the UK due to its recent exit from the EU. For now, banking and financial market sectors in the UK have been directed to comply with obligations and requirements provided by the BoE and/or the FCA.[154]

The UK's decision to exclude FIs in its implementation of the NIS Directive appears to stem from concerns relating to the over-regulation of FIs where increasing regulatory and administrative costs may result in operational failure. In this regard, UK Finance[155] note that overlapping initiatives from various authorities involved in financial regulation can often lead to unnecessary compliance and implementation costs, leading to less performance in other significant services.[156] Without specific reference to considerations of overlapping cybersecurity regulations in the sector, the consequences of these cannot be

[152] Explanatory Memorandum to the Network and Information Systems Regulations 2018 No. 506, para 4.4.
[153] European Commission, Report from the commission to the European Parliament and the Council: Assessing the consistency of the approaches taken by Member States in the identification of OES in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems (28 October 2019) para 2.7.
[154] Department for Digital, Culture, Media, and Sport, 'Security of Network and Information Systems Public Consultation' (August 2017) 7.
[155] UK Finance is the UK banking and financial industry trade group delivering credit, banking and payment support services to about 300 firms.
[156] HM Treasury, 'Financial Services Future Regulatory Framework Review Call For Evidence: Regulatory Coordination UK Finance Response' (18 October 2019) paras 21 - 24 <https://ukfinance.org.uk/system/files/HMT%20call%20for%20evidence%20on%20regulatory%20coordinthation%20-%20UK%20Finance%20response.pdf> accessed 28 December 2020.

speculated. Given that, we compare security obligations under the DPA 2018 and NIS Regulations 2018 to shed more light on the EU's argument that the current scope of application of the NIS Directive is limited. This is based on the understanding that almost, if not all kinds of personal data are often conveyed or processed through networks and information systems. This comparison is presented in the table below:

	DPA 2018	NIS Regulations 2018
Concerns	Personal Data	Security of network and information systems
Applicable to	Data controllers and processors	OES and Digital Service Providers (DSPs) (with certain exceptions)
Security Measures	must be "appropriate" to the relevant risks (Sections 55)	must be "appropriate" and proportionate to the relevant risks (Regulation 10)
Risk Focus	focus on 'personal data' referring to information associated with an "identified or identifiable living individual" (Sections 1 and 3(2)).	focus on electronic communications network, systems, devices, any digital data stored, processed, retrieved or transmitted by those systems. (Regulation 1(2))
Regulator	ICO (Part 5)	Relevant competent authorities for OES (Regulation 3)
Duration of Notification	without undue delay, a 72-hour deadline 'where feasible', or a later notification after 72 hours providing reasons for the delay (Section 67)	without undue delay and a 72-hour deadline (Regulation 11(3)(b) for operators of essential services).
Sanctions	Maximum penalties in the range of £20,000,000 or 4% of the firm's total annual global revenue, or standard maximum of £10,000,000 or 2% of the	Penalties in the range of £1,000,000 to £17,000,000 may be imposed (Regulation 18(6)).

	firm's total annual global revenue; in the preceding financial year, may be imposed (Section 157).	

Table 4-6 *Comparison of Security Standards Under NIS Regulations 2018 and DPA 2018*

Similar to the DPA 2018, the NIS Regulations 2018 contain obligations which have direct risk management implications for institutions, like FIs, to ensure security of its network and information systems. Regulation 10 (1) and (2) provides that operators of essential services:

> must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies [and]. . . to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.

The interpretation of the term "appropriate" is to be taken as meaning the same thing with that of the DPA in a technical sense. Proportionality, on the other hand, means that the security measures deemed appropriate must reflect a risk-based approach, where resources and techniques are tailored according to risk levels. This brings into view the discussions on risk prioritisations in Chapter 3 and the ways in which such prioritisations, achieved only through a continued process of calculations, may facilitate the design of appropriately proportionate security measures. Through repeated calculations, reflexive learning is produced, and better performance may be achieved through systems of knowledge. The Regulation also requires that security measures adopted must take into consideration "the state of the art"[157] towards achieving security objectives. In this regard, we observe a principles-based, non-prescriptive approach to cybersecurity which recognises the evolving landscape of cybersecurity threats.

On the subject of risk focus, we observe limitations as the DPA focuses mainly on risks to processing of personal data, while the NIS Regulations extend their focus beyond

[157] Network and Information Systems Regulations 2018, Regulation 10(3).

networks, systems and devices to *any* digital data, thus bringing personal data within the scope of their interpretation. Arguably, the NIS Regulations will provide a more significant and overarching framework than the DPA for the financial sector whose operations involve the direct and indirect processing, management and storage of large sensitive/personal customer data across devices, networks and systems.

With regards to incident notifications, the NIS Regulations offer a more stringent approach to notification than the DPA, as it does not make provisions for later reports, supported with reasons. That being said, it appears that such requirement may involve large compliance costs which FIs seek to avoid. Notification involves an assessment of a number of factors towards ascertaining incidents of significant impacts all within a space 72 hours, which sometimes may be impractical. For this reason, FIs may either burden competent authorities, like the FCA and PRA with expending resources in distinguishing material from immaterial incidents or underreport cyber incidents. In particular, where an institution is found liable for data breaches due to failing IT systems, concerns over double jeopardy may arise and fear of facing highly substantial fines may discourage voluntary reporting. It is believed that awareness of penalty scales or effective enforcement of sanctions on offending institutions may incentivise a change in behaviour in non-offending institutions. Although, this will rarely be the case as the Regulations, taking into account responses from the consultation paper, sets out a provision requiring that the enforcement authority, prior to an enforcement action, must take into account enforcement liabilities due the infringement arising under another enactment.[158]

While it may be argued that security risk management and notification provisions under the PSRs 2017 represent sufficient supplementary guidelines to the DPA 2018 for FIs, the financial services sector must be reminded that these guidelines are directed at PSPs. Arguably, PSPs may include banks and even provisions of the PSRs may be broadly interpreted to do so. Viewed differently, Principle 11 of the FCA Handbook appears to satisfy the first determining factor under notification requirements for OES under the NIS Regulations[159] by requiring reports of incidents which affect a large number of customers. It

[158] Network and Information Systems Regulations 2018, Regulation 23.
[159] Network and Information Systems Regulations 2018, Regulation 11(2)(a); "the number of users affected by the disruption of the essential service".

however makes no provision for the duration and geographical reach of the incident[160] stated under the Regulations. Both factors are of great significance as the duration of the breach might impact on the response and recovery time from the breach and the geographic reach takes into account the globality of cyber risks identified in Chapter 3. At this point, the UK Government's justification for intentionally or unintentionally depriving the financial sector of the 'state of art' security provided for under the NIS Regulations is unclear and it is only hoped that relevant cybersecurity requirements for FIs are brought up to speed with provisions of the NIS Regulations.

Regarding enforcement, as this discussion makes clear, there has not been any evidence of a breach of the abovementioned legislation by FIs nor related criminal enforcement actions. The majority of enforcement in the area of financial cybersecurity is initiated by delegated authorities in form of civil penalties for breach of sector-wide principles. In this sense, if approved, the complete and thorough implementation and enforcement of the NIS Regulations by FIs will take time and may more likely involve regularly reviews due to requirements of proportionality and appropriateness. Overall, it is noteworthy, that legislation do provide standards by which UK FIs develop their organisational frameworks and set best practices.[161]

4.8 Possible Challenges to Reflexivity in UK FI Cybersecurity Regulation

Perceived Duplication of Responsibilities in Regulation

The overlapping remits of the different regulators and government authorities have been a longstanding criticism of the financial sector. In particular, these concerns were highlighted by Fisher QC who observed problems with investigation and prosecution of crimes owing to unwarranted duplication of responsibilities, capabilities and resources between the authorities.[162] Lastra et al note that such duplication of functions or incompatibility in regulation may pose significant risks in the event of a crisis response.[163] A cohesive structure

[160] Network and Information Systems Regulations 2018, Regulation 11(2)(b) and (c).
[161] Financial Conduct Authority 'Cybersecurity - industry insights' (March 2019) 6.
[162] Jonathan David Fisher, *Fighting fraud and financial crime: a new architecture for the investigation and prosecution of serious fraud, corruption and financial market crimes* (Policy Exchange 2010).
[163] P. Conti-Brown and R.M. Lastra, *Research Handbook on Central Banking* (Edward Elgar Publishing 2018) 152.

is important for coordination and information sharing as through these, practices, standards and insights are all produced and reproduced in processes, thus reinforcing the value of reflexivity.

The current arrangement for cyber incident notifications in the UK financial sector may give rise to the unintentional duplication of responsibilities where there is insufficient standard coordination of tasks amongst regulators. The FCA in its Good Cybersecurity Factsheet, notes different cyber incident reporting requirements to different regulators and government bodies. For fixed and flexible firms, report is to be made to the FCA; for dual-regulated firms, report is to be made to both the FCA and PRA; and for data breaches, report is to be made to the ICO.[164] The notification of data breaches to the ICO is within the context of the DPA 2018. However, in the context of the NIS, reports made by dual-regulated firms could cause regulatory confusion and considerably increase regulatory costs, where there is improper coordination among authorities.

The UK Finance in its report on the Financial Services Future Regulatory Framework Review, notes that institutions observe an absence of regulatory coordination amongst the relevant authorities: by their operations in the same policy fields without aligning their actions and their imposition of different regulatory burdens on institutions simultaneously.[165] In fact, there is further room for overlap of regulatory functions as OES will generally be data controllers and sometimes processors and oftentimes, instances of violations under NIS Regulations will often involve personal data breaches. The ICO recognises this[166] and notes that in such instances, competent authorities are to "consult and co-operate with the Information Commissioner when addressing incidents that result in breaches of personal data" in accordance with Regulation 3(3)(f).

With the unintentional duplication of roles, there comes various risks particularly the risk of crimes not being adequately investigated or prosecuted, thus creating the need to clarify the remits/mandates of each body. Currently, neither the FCA nor the PRA have

[164] Financial Conduct Authority, 'Good cybersecurity - the foundations' (2017).
[165] HM Treasury, 'Financial Services Future Regulatory Framework Review Call for Evidence: Regulatory Coordination UK Finance Response' para 36.
[166] Information Commissioner's Office, 'NIS and the UK GDPR' <https://ico.org.uk/for-organisations/the-guide-to-nis/nis-and-the-uk-gdpr/> accessed 6 January 2021.

specific statutory responsibilities in enforcing the DPA and NIS Regulations 2018. At most, both authorities, by virtue of their mandates are able to extend their remits to cover cybersecurity. Nevertheless, the issue of overlapping functions is recognised by the agencies themselves who reiterate that investigations will only be initiated by the agency or agencies with the most relevant functions and powers.[167] Moreover, this has been confirmed in recent cases where the FCA and PRA have avoided duplication of roles and coordinated operations in investigating and imposing sanctions for IT failings.

Rushed Risk Management Processes

Another possible challenge to reflexivity in cybersecurity regulation arises from the huge burden placed on institutions to fit IT changes within small timeframes due to regulatory objections to disruption of services.[168] The likely result of such changes may involve a doubled increase in the risks to the security and resilience of operations. Where IT changes are rushed, the learning process is withered and the time for FIs to take in new knowledge becomes limited, thus hampering the reflexivity ideal. The concerns of regulators are understood as risk concerns regarding data loss and breaches, financial losses, availability of systems, slow recovery times and operational resilience. Nevertheless, risk management should effectively involve a sustained exercise. As such, it is suggested that institutions affected by regulatory oppositions consider interim transitional adjustments in advance of comprehensive remediation frameworks.

Underreporting of Cyber Incidents

Evidence has shown that financial services firms underreport IT and cyber-related incidents.[169] That is, FIs intentionally avoid providing complete information on cyberattacks that could influence risk assessment due to concerns that disclosures will expose weaknesses

[167] Financial Conduct Authority, 'Enforcement Guide' Annex 2, para 7 <https://www.handbook.fca.org.uk/handbook/document/EG_Full_20160101.pdf> accessed 6 January 2021.
[168] HM Treasury, 'Financial Services Future Regulatory Framework Review Call for Evidence: Regulatory Coordination UK Finance Response' para 40.
[169] Financial Conduct Authority, 'Cyber and Technology Resilience: Themes from cross-sector survey 2017/2018' (November 2018) para 2.10.

in their cybersecurity systems. These concerns include a tarnished image, financial losses[170]or a perception that incidents are too immaterial to be reported.[171]

Problems of underreporting were highlighted in the *Online Fraud* survey by the NAO.[172] The risk posed by underreporting is greater than the cost of reporting. Specifically, firms who comply with reporting obligations are able to improve the perception and assessment of cyber threat landscape. Scholars have argued that the underreporting of cyber incidents encourages cybercriminal behaviour in view of the perception that the longevity of crime is in its low visibility.[173]

A major issue associated with underreporting is the uncoordinated response by banks to fraud. The inaccuracy of APP scam data in 2016, noted by the Payment Systems Regulator[174] is one of the reasons why the analysis of risk trends in the earlier section commenced from the year 2017. The data inaccuracies revealed the failure of FIs to live up to their obligations under previous laws, set out in Article 10(4) of the EU PSD 1[175] and Regulation 6(5)(b) of the UK PSR 2009, which states that PSPs must establish "effective procedures to identify, manage, monitor and report *any* risks to which it might be exposed". 'Any risks' appear to cover security risks which have the tendency to significantly disrupt the services of PSPs. In essence, FIs were under a duty to report accurately and appropriately, data relating to APP scams. Given that, the passive approach taken by FIs raises questions as to the extent to which reflexivity is followed in terms of implementation of regulations the sector.

---

[170] T.J. Holt and A.M. Bossler, *Cybercrime in Progress: Theory and prevention of technology-enabled offenses* (Taylor & Francis 2015) 107.
[171] I.R. Management Association, *National Security: Breakthroughs in Research and Practice: Breakthroughs in Research and Practice* (IGI Global 2019) 335.
[172] National Audit Office, 'Online Fraud' (30 June 2017) para 3.14 <https://www.nao.org.uk/wp-content/uploads/2017/06/Online-Fraud.pdf> accessed 13 August 2019.
[173] Audrey Guinchard, 'Between hype and understatement: reassessing cyber risks as a security strategy' (2011) 4 Journal of Strategic Security 75, 80 and Marcus K Rogers, 'The psyche of cybercriminals: A psycho-social perspective', *Cybercrimes: A Multidisciplinary Analysis* (Springer 2011) 228.
[174] Payment Systems Regulator, 'PSR kick-starts industry-wide effort to tackle payment scams' (16 December 2016) <https://www.psr.org.uk/psr-publications/news-announcements/psr-kick-starts-industry-wide-effort-tackle-payment-scams> accessed 28 April 2018.
[175] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC, and 2006/48/EC.

Current regulations under Article 95 and 96 of the EU PSD 2[176], and Regulation 99 of the PSR 2017 provide specific reporting requirements for operational and security risks, to which the old law makes no reference. In addition, the requirement under Regulation 98(1) of the PSR 2017 to "establish and maintain effective incident management procedures" poses maintenance requirements identical to the reflexivity process towards developing cyber incident management procedures.[177] Under these new laws, FIs risk facing enforcement actions in the form of public censures and penalties, directly issued by the FCA who is designated with specific statutory responsibilities under the regulations.[178]

Information Asymmetries

Finally, there are severe consequences associated with information asymmetries in a reflexive cybersecurity regulation. It has been reported that there are information asymmetries between the financial services sector, government and law enforcement agencies[179] which may be partly due to the absence of formal requirements for reporting or sharing of fraud reports by FIs with the government or the police.[180] Issues such as this reinforce the argument towards implementing the NIS regulations in the financial sector. The current design for information sharing is by way of a guide from the FCA encouraging firms to partake in the combined industry and Government scheme for exchanging cyber-threat intelligence; the Cyber Security Information Sharing Partnership (CiSP) towards understanding the sector's cyber incident response plan as well as the relevant threat landscape.[181]

Where regulators receive inadequate information about cybersecurity incidents, they may be likely to implement regulations inadequately that is, in the absence of regular supervision through cyber resilience exercises. In the same vein, where there are asymmetries in sector-wide cyber incident information sharing, there will not be a comprehensive understanding of the threat landscape, and where some FIs make cybersecurity risk management decisions, these might be poor not be fully informed. The Raphael's case,

[176] Directive (EU) 2015/2366.
[177] Payment Systems Regulations 2017, Regulation 98(1).
[178] Payment Systems Regulations 2017, Regulations 110 and 111.
[179] National Audit Office, 'Online Fraud' (30 June 2017) para 3.14.
[180] House of Commons Committee of Public Accounts, 'The Growing Threat of Online Fraud: Sixth Report of Session 2017-19' (6 December 2017) 7 <https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/399/399.pdf> accessed 30 April 2018.
[181] Financial Conduct Authority, 'Good cybersecurity - the foundations' (2017).

provides instances where an FI, while failing to exercise due care, skill and diligence, may make poorly informed security choices in an outsourcing arrangement, if it unreasonably relies on its sub-contracted processors submission of possible risks to the services provided. Constant monitoring, communication and review of IT processes are steps which can be engaged by FIs to manage the problems of information asymmetry.

4.9 Conclusion

Viewing reflexivity as an element of cyber risk management emphasises the importance of an autopoietic system, one which changes/adapts in this case, based on the cybersecurity risk profile. With this view, firms, regulators and relevant industry partners represent components of the system characterised by their interdependence and replication of learning processes, with the overall objective of promoting stability and cyber risk resilience in the financial system.

Three relevant conclusions may be drawn from this chapter. First, that the poor compliance of firms with cyber incident reporting requirements indicates poor learning on the part of the financial services sector to embrace reflexivity, possibly owing to the inadequacy of specific statutory responsibilities on FIs and regulators alike. Moreover, we observe the government's reluctance to impose relevant statutory obligations, affording it lower priority than incentivising the sector. Softening the implementation of regulations like the NIS is short sighted and obstructs the development of effective cybersecurity compliance culture in FIs, integral to both internal/external control processes, which if performed adequately, may help to assist and sustain effective cyber risk management processes.

The second conclusion is that multiple regulators/supervisors may hinder the effectiveness of cyber risk regulatory frameworks. While there is to an extent certainty on the roles and responsibility of regulators in the UK financial sector, evidence has shown that overlapping mandates, structural gaps and too many guidelines issued by various authorities may prevent effective cyber regulation. Hence, clarifying regulatory responsibilities will help overcome the challenges posed by regulatory duplication.

Furthermore, third-party outsourcing arrangements may bring about certain complexities where there has been a breach of customers' data. Indeed, third-party vendors

have been classified as 'key vulnerabilities in an institution's supply chain,'[182] which are exploited as tools in a cyberattack to get to the institutions themselves. To assess and manage risks posed by third-party vendors, institutions may monitor vendor profiles and rating, perform due diligence, track and assess performance[183] as well as periodic assessment of risks posed by a third party.[184] Allied to this, relevant standards governing third-party management of data or security breaches should be duly implemented.

The UK's cyber risk management framework is one which has without a doubt proven to be effective for addressing flaws in cybersecurity frameworks of individual firms, especially those relating to IT failings. Nevertheless, it must be noted that cyber risk regulation is a collective responsibility which must not only be left to the regulators but extended to the regulated entities who must cooperate to proactively monitor, manage and respond to threats.

[182] M. Gehem and others, *Assessing Cyber Security: A meta analysis of threats, trends, and responses to cyber attacks* (The Hague Centre for Strategic Studies 2015) 50.
[183] W. Tian, *Commercial Banking Risk Management: Regulation in the Wake of the Financial Crisis* (Palgrave Macmillan US 2016) 355.
[184] P.H. Gregory, *CISM Certified Information Security Manager Practice Exams* (McGraw-Hill Education 2019) 172.

Chapter 5. Case Study United States

5.1 Introduction

Ranked as the 3rd highest internet using country in the world with about 312 million internet users[1], the US is reported as the country with the highest average data breach cost estimated at $8.64 million in 2020, an approximately 5.5% increase from $8.19 million in the year 2019[2]. Indeed, research has shown that its financial services sector faces an increasing, multifaceted threat of cyberattack incurring millions of losses both to institutions and customers.[3]

The recent cyberattack on Equifax[4] (2017) show the many complexities surrounding a cyberattack, including the impact to all parties involved. In the case, there was a cybersecurity breach affecting 150 million consumer records, involving sensitive data. The breach is currently estimated at $1.4 Billion. As it is a large organisation processing millions of data, questions arose regarding the adequacy of their cybersecurity risk management frameworks and the efficacy of legislation and regulation in data breach prevention and management.[5] Thus, probing the regulation of self-regulation through state intervention.

The US Department of Justice considers law enforcement as a fundamental component in tackling cyber threats. It notes that "Individual efforts, while unquestionably important, simply are not enough. Law enforcement is a necessary part of combatting cyber threats. Disrupting and deterring the next attack is far more effective than merely trying to avoid becoming the next victim."[6] The phrase disrupting and deterring highlight a process,

---

[1] T.L. McPhail and S. Phipps, *Global Communication: Theories, Stakeholders, and Trends* (Wiley 2019) 83.
[2] IBM Security, 'Cost of a Data Breach Report 2020' 12 <ibm.com/downloads/cas/RZAX14GX> accessed 10 May 2021. IBM Security, 'Cost of a Data Breach Report 2019' 5 <https://www.ibm.com/downloads/cas/ZBZLY7KL> A 3.5% increase from the year 2018, estimated at $7.91 million in 2018. See IBM Security, '2018 Cost of a Data Breach Study: Global Overview' 5 <https://www.ibm.com/downloads/cas/861MNWN2> accessed 10 September 2019.
[3] Tim Maurer, Ariel Levite and George Perkovich, 'Toward a global norm against manipulating the integrity of financial data' (2017) Economics Discussion Papers (7 March 2017) <https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403> accessed 10 July 2020.
[4] US Senate Equifax Report.
[5] David Zaring, 'Equifax Deal: Credit Agencies Must Change How They Manage Data' (30 July 2019) <https://knowledge.wharton.upenn.edu/article/equifax-settlement-key-takeaways/> accessed 15 July 2020.
[6] US Department of Justice (US DOJ), 'Deputy Attorney General Rod J Rosenstein Delivers Remarks at the Cambridge Cyber Summit Boston' (4 October 2017) <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit> accessed 10 July 2020.

one that is continuous, reflexively governed, and possibly involving a form of monitoring and re-monitoring towards learning mechanisms for interrupting or preventing a cyberattack.

This chapter aims to contribute to research on the effectiveness of risk management frameworks in FIs for the identification, assessment, control and review of cybersecurity risks by exploring the case study of two major banks in the US. In doing so, the chapter investigates the effectiveness of cyber risk regulation and supervision in US FIs and questions the applicability of the regulatory frameworks and the role of regulators and law enforcement authorities in enforcing the accountability of financial institutions, deterrence and punishment of misconduct. In particular, we identify criminal justice responses and self-regulatory responses to address an important argument that there is no one-size-fits-all approach when it comes to cyber risk regulation in the financial sector. As explored in Chapter 4, it seeks to validate the regulatory co-existence hypothesis by exploring the extent to which the government, through regulatory authorities may intervene in self-regulation.

It is the purpose of this chapter, therefore, to outline the development of the financial sector cybersecurity regulatory framework in the USA and provide an understanding of current self-regulatory approaches and applicable criminal justice responses to self-regulatory failures and suggest recommendations on how both responses may co-exist to ensure effective security and resilience to cyber threats.

5.2 Institutional Framework of the US Financial System

The US operates a decentralised system structure in which there is a central authority and independent units across its twelve regions owned by member reserve banks towards ensuring a separation of responsibilities between institutions for objectives that are national in scope. Generally, such multi-institutional framework consisting of regulation and supervision by federal and state authorities may be argued to be a proportionate approach to the multi-layered nature of threat faced by banks in the US. Moreover, majority of the key US financial regulators were introduced by statute in response to a crisis or incidence in the financial

markets. Despite this, the framework has been regarded as a "patchwork", causing considerable disparities in the regulation of cyberspace.[7]

The US banking system consists of various types of institutions namely commercial banks, credit agencies, savings institutions/thrifts and other specialised institutions. This system is commonly referred to as the "dual banking system" due to regulations which exist at both federal and state level. In some cases, this form of regulation has been regarded as overlapping and intricate in which too many regulators bear responsibilities for regulation and supervision.[8] Although, banks are able to choose which one of the three federal banking agencies is to exercise key regulatory power over them.

The Federal Banking Authorities expect the board of directors to be held accountable and assume responsibility for any such risk levels taken by their institution.[9] As such, institutions including those in the financial services sector are required to develop and implement their own cybersecurity risk frameworks in accordance with the risks they face, while being supported by the Department of Homeland Security and other relevant agencies to guarantee an adequate level of security across businesses and address systemic risks across institutions.[10]

The US adopts a functional and institutional approach to financial regulation i.e., regulation based on the type and function of the institution.[11] Regulation and supervision of depository institutions at a federal level is primarily undertaken by four federal agencies and several other agencies which regulate different aspects of the financial system and regulated at state level by state regulators where they are chartered or licenced. Regulators relevant to the discussion at hand, are represented in the chart below.

[7] Kristin N Johnson, 'Managing cyber risks' (2015) 50 Georgia Law Review 547, 576.
[8] R. Bosch and R. Bösch, *Banking Regulation: Jurisdictional Comparisons* (Thomson Reuters 2012) 379.
[9] International Monetary Fund. Monetary and Capital Markets Department, *United States: Financial Sector Assessment Program-Detailed Assessment of Observance on the Basel Core Principles for Effective Banking Supervision* (International Monetary Fund 2015) 209.
[10] US Department of Homeland Security (DHS), 'Cybersecurity Strategy' (15 May 2018) 8 <https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf> accessed 15 August 2018.
[11] A. Gottesman and M. Leibrock, *Understanding Systemic Risk in Global Financial Markets* (Wiley 2017) 86.

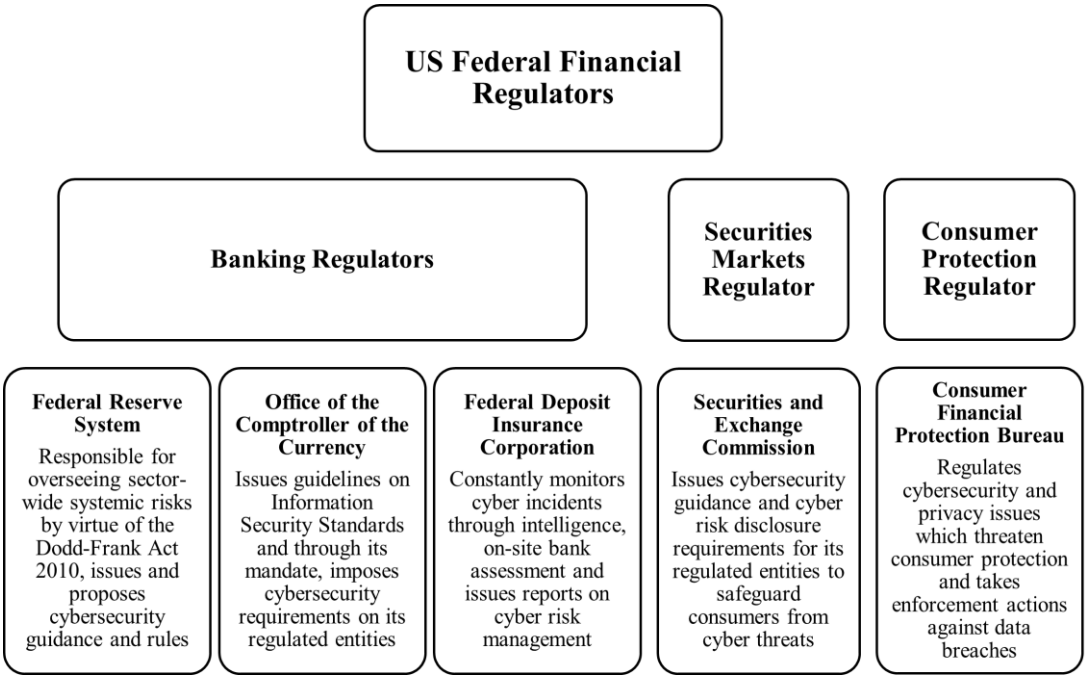

Figure 5-1 *US Financial Regulatory Approach to Cyber Risk Regulation*

The Federal Reserve System or Board

The Federal Reserve System (FRS) was introduced under the Federal Reserve Act 1913 to address instability in the financial services sector resulting from the banking panic. The FRS is designated as the primary regulator for all financial services institutions which the Oversight Council presents as systematically significant and has the power to carry out safety and soundness assessments on the institutions which it regulates.

As the central banking authority and as a member of the Federal FIs Examinations Council, the FRS may propose rules and issue joint statements/guidance on cybersecurity for FIs to mitigate abrupt systemic effects of a cyber-attack or a large-scale disruption on critical financial markets. For example, the *2016 Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards* amongst others, proposes an integration of business-wide cyber risk management within the independent risk management function and a

requirement for regular business units to review, on a constant basis, the cyber risks present in its operations.[12]

Office of the Comptroller of Currency

The Office of the Comptroller of Currency (OCC) was introduced as a part of the US Treasury Department by the National Currency Act 1863. The OCC is responsible for the issuance of charters for national banks and federal savings institutions. The OCC's cyber-related function lies in ensuring the safety and soundness of the federal banking system.

The OCC prioritises cybersecurity and operational resiliency in its *Operating Plan for the Fiscal Year 2020* as a topmost risk area[13] and conducts compliance and operational risk workshops to discuss operational risks like cybersecurity and governance, and key components of an effective risk management strategy.[14] Through its National Risk Committee (NRC), it issues the *Semiannual Risk Perspective*, a report which covers key and current risk areas facing banks and how these risks threatens its regulatory objectives. Specifically, in its 2019 report[15], it emphasises third-party providers and technological innovations as major risk issues. In particular, it notes the lack of expertise, ineffective implementation and weak control systems in relation to third parties.[16]

The OCC also encourages partnership with the Financial Services Information Sharing and Analysis Center (FS-ISAC), the U.S. Computer Emergency Readiness Team (US-CERT) and other information-sharing bodies, to gather information on cyber threats and

[12] Federal Reserve System (FRS), 'Advance Notice of Proposed Rulemaking - Enhanced Cyber Risk Management Standards' (19 October 2016) 27 <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20161019a1.pdf> accessed 15 August 2018 (FRS Enhanced Cyber Risk Management Standards).
[13] Office of the Comptroller of the Currency (OCC), 'Fiscal Year 2020 Bank Supervision Operating Plan' <https://www.occ.gov/news-issuances/news-releases/2019/2019-111a.pdf> accessed 7 October 2019.
[14] OCC, 'OCC Hosts Compliance and Operational Risk Workshops in Los Angeles' (*News Release 103*, 9 September 2019) <https://www.occ.gov/news-issuances/news-releases/2019/nr-occ-2019-103.html> accessed 7 October 2019.
[15] OCC, 'Semiannual Risk Perspective Spring 2019' 12 <https://www.occ.treas.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-spring-2019.pdf> accessed 8 October 2019.
[16] ibid 1.

vulnerabilities to themselves as well as third-party providers and develop their risk management frameworks to address this.[17]

Federal Deposit Insurance Corporation

The Federal Deposit Insurance Corporation was introduced under the Banking Act 1933.[18] The FDIC is an independent federal agency responsible for the examination and supervision of over half of US FIs. The FDIC is the primary regulator of state-chartered banks who are non-members of the FRS and state-chartered savings institutions. The FDIC exercises its authority by assessing federally insured depository institutions to oversee and implement safety and soundness.[19]

The FDIC also supervises cybersecurity in FIs through regulatory reports and shared intelligence. In addition, it has various resources developed to assist banks with responding to cyber-related incidents and enhancing cybersecurity awareness. This include, the "Cyber Challenge" cybersecurity preparedness exercise, a cybersecurity awareness training program for staff, management and institutions under its supervision.[20]

Securities and Exchange Commission

The Securities and Exchange Commission was introduced under the Securities Exchange Act 1934 and is primarily responsible for regulating the securities markets. The SEC's primary objective is the protection of investors, sustenance of fair, organised, and effective markets, and aiding capital creation.

In a speech delivered by the SEC's former Commissioner[21], the implementation of cybersecurity policies were viewed as significant, particularly its incorporation in a Board's

[17] OCC, 'Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29' (5 March 2020) < https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html> accessed 15 July 2020.
[18] Supplanted by the Federal Deposit Insurance Act 1950.
[19] CRS, 'Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework' (Updated 10 March 2020) 8 <https://fas.org/sgp/crs/misc/R44918.pdf> accessed 10 July 2020.
[20] Federal Deposit Insurance Corporation (FDIC), 'A Framework for Cybersecurity' (2015) 8 <https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin15/si_winter2015-article01.pdf> accessed 10 October 2019.
[21] Luis A Aguilar, *Boards of directors, corporate governance and cyber-risks: Sharpening the focus* (2014) <https://www.sec.gov/news/speech/2014-spch061014laa> accessed 10 October 2019.

overall risk oversight. That is, emphasising the fiduciary duties of the corporate board as an important factor in cyber risk management and mandating financial institutions, investment companies and broker-dealers to place responsibility on one or more staff for the coordination of its cybersecurity programme. This view, consistent with the argument in Chapter 3 on corporate liability for cybersecurity risks, has also been echoed in policy studies by the World Bank noting that the Board's role should not be limited to adopting cybersecurity guidelines but ensuring their effective implementation.[22]

Further, the SEC conducts a program on regulated entities through the Office of Compliance Inspections and Examinations (OCIE) to issue risk alerts such as those covering cybersecurity initiatives.[23] Also, it enforces a number of laws and regulations containing cybersecurity requirements including the Sarbanes-Oxley Act 2002 and the Privacy of Consumer Financial Information (Regulation P). The SEC is granted enforcement powers to initiate civil actions against institutions found to be in breach of the law. Through this, it may recommend a case to the Justice Department for criminal prosecutions. As part of its efforts to address cybersecurity threats and attacks, the SEC established a Cyber Unit under its Enforcement Division concerned with cyber-related violations in or against its regulated entities.[24]

Consumer Financial Protection Bureau

Prior to the 2008 crisis, consumer financial protection was a shared responsibility between several federal agencies and financial regulators. The Consumer Financial Protection Bureau (CFPB) was introduced under Title X of the Dodd-Frank Act 2010 for the supervision of consumer financial protection and enforcement of federal consumer protection legislation for depository and non-depository FIs, following the 2008 crisis.

The implementation of cybersecurity standards that protect customer data, products and services is an aspect of consumer protection. In this regard, the CFPB has mandates

[22] Aquiles A Almansi, 'Financial sector's cybersecurity: regulations and supervision' (2018) The World Bank 11.
[23] Office of Compliance Inspections and Examinations (OCIE), US Securities and Exchange Commission (SEC), 'National Exam Program: Examination Priorities for 2016' 3 <https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf> accessed 16 August 2018.
[24] SEC, 'SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors' (25 September 2017) <https://www.sec.gov/news/press-release/2017-176 > accessed 16 September 2019.

within relevant financial legislation containing cybersecurity requirements, such as the Fair and Accurate Credit Transactions Act 2003 in establishing identity theft rules and the Gramm-Leach-Bliley Act (GLBA) 1999 in issuing privacy regulations.[25] Further, by virtue of its authority under the Dodd Frank Act 2010, the CFPB has in recent times implemented its investigation and enforcement powers to cover privacy-related and data security breaches, such as in the *Equifax* case.[26]

Regulatory Coordination

In order to ensure an effectively coordinated regulation of the financial system, some of the authorities identified in ***Figure 5-1*** collaborate to develop standard reporting systems and oversee systemic threats and risks in relevant FIs.

Financial Stability Oversight Council

In response to the 2008 financial crisis which revealed a failure in financial regulation and supervision, the Dodd-Frank Act 2010 makes significant changes to the regulatory structure of the financial system and establishes new bodies discussed in later sections, including the Financial Stability Oversight Council (FSOC). The FSOC is responsible for detecting potential systemic risks which threaten the stability of the financial system, and refer to the FRS for supervision, institutions which it has identified as posing risks which may result in significant losses and devastating consequences for the financial system.[27]

The FSOC publishes an annual report risk factors in the financial system, major financial and regulatory developments and proposing recommendations to eliminate risk factors. In its 2019 Annual Report, the report outlines vulnerabilities in the financial system namely data breaches, malware attacks and ransomware attacks, which results in potentially

[25] Congressional Research Service (CRS), 'Financial Services and Cybersecurity: The Federal Role' (Updated 23 March 2016) 6 <https://crsreports.congress.gov/product/pdf/R/R44429> accessed 10 December 2020 (CRS Financial Services and Cybersecurity).
[26] Consumer Financial Protection Bureau (CFPB), 'Bureau Of Consumer Financial Protection v Equifax Inc: Stipulated Order For Permanent Injunction And Monetary Judgment' (23 July 2019) https://files.consumerfinance.gov/f/documents/cfpb_equifax-inc_stipulated-order_2019-07.pdf> accessed 10 December 2020.
[27] United States Congress House, Committee on Financial Services and Subcommittee on Oversight and Investigations, *Oversight of the Financial Stability Oversight Council: Hearing Before the Subcommittee on Oversight and Investigations of the Committee on Financial Services, U.S. House of Representatives, One Hundred Thirteenth Congress, Second Session, September 17, 2014* (US Government Printing Office 2015) 39.

significant costs and losses running over billions of dollars.[28] Some of the FSOC's recommendations include a strong and effective cybersecurity monitoring and assessment of third-party service providers, creation of partnerships between FIs and the government, including authorities to enhance cyber threat intelligence sharing and harmonisation of approaches.[29]

Federal Financial Institutions Examination Council

The Federal Financial Institutions Examination Council (FFIEC) was introduced under statute in 1979[30] to be responsible for coordinating the regulation of lending institutions at federal level. The FFIEC consists of representatives from the FRS, OCC, FDIC, CFPB, National Credit Union Administration, and the State Liaison Committee to ensure uniformity in the examination of institutions and to administer safety and soundness regulations.

The FFIEC prescribes a single set of reporting forms for the examination of FIs and makes proposals for ensuring uniform supervision. Federal financial institution examiners assess the risks of FIs using guidance provided in its *Information Technology Examination Handbook*[31]. Occasionally, the FFIEC also sets out guidance and resources on organisations which FIs collaborate with for conducting assessments, exercises, sharing intelligence and reporting/responding to cybersecurity incidents.[32] Such organisations include the DHS, FBI's Internet Crime Complaint Center and the Financial Crimes Enforcement Network (FinCEN).

Due to the increasing reliance on technology and the evolving cyber threat landscape in the US, FIs have in some cases outsourced the processing of data to third parties. As a result, it became important to issue a comprehensive cybersecurity guidance on risk management practices to be followed by FIs and services provided by third parties as well as

[28] Financial Stability Oversight Council (FSOC), '2019 Annual Report' (December 2019) 115 <https://home.treasury.gov/system/files/261/FSOC2019AnnualReport.pdf> accessed 12 July 2020.
[29] ibid 9.
[30] Financial Institutions Regulatory and Interest Rate Control Act of 1978 (P.L. 95- 630, 92 Stat. 364).
[31] Federal Financial Institutions Examination Council (FFIEC), 'Information Technology Examination Handbook' <http://ithandbook.ffiec.gov/it-booklets/information-security.aspx> accessed 20 May 2019 (FFIEC IT Examination Handbook).
[32] FFIEC, 'Cybersecurity Resource Guide for Financial Institutions' (October 2018) <https://www.ffiec.gov/press/pdf/FFIEC%20Cybersecurity%20Resource%20Guide%20for%20Financial%20Institutions.pdf> accessed 20 May 2019 (FFIEC Cybersecurity Resource Guide).

guidance on how they are reviewed. This guidance was contained in the IT Handbook issued by the FFIEC in 2003.[33]

In 2014, the FFIEC and OCC led an interagency Cybersecurity Assessment by launching a program to assess the cybersecurity readiness of over 500 member institutions.[34] The results of the assessment, which was shared into two reports, suggested key issues for FIs to consider, made available resources for support and urged FIs to join the FS-ISAC, to enhance the notification and sharing of information on cyber-threats and vulnerabilities.[35]

The FFIEC also introduced a Cybersecurity Assessment Tool in 2015, by which FIs and certain regulated financial entities, may voluntarily adopt in assessing their cybersecurity risks and ascertain their cybersecurity preparedness.[36] This assessment, discussed later in the chapter, provides FIs with processes which may be repeated and accessed to enhance risk management frameworks and cybersecurity capabilities. Meanwhile, the FFIEC also advices FIs on responsibilities of board and senior management to assess the adequacy of their detection, response and recovery capabilities against their inherent risk profiles.[37]

Financial Services Information Sharing and Analysis Center

The FS-ISAC similar to the UK CiSP, was formed in 1999 to coordinate the sharing of information relating to cybersecurity threats and management amongst security experts in the financial services sector. There are a number of ISACs in other jurisdictions to enhance partnership between the government and industry.

The FS-ISAC's responsibility includes, but is not limited to, gathering and sharing of cyber threats, risks and vulnerabilities information; assessment of information collected to

[33] FRS Enhanced Cyber Risk Management Standards, 9.
[34] FFIEC, 'FFIEC Launches Cybersecurity Web Page, Promotes Awareness of Cybersecurity Activities' (24 June 2014) <https://www.ffiec.gov/press/pr062414.htm> accessed 16 August 2018.
[35] FFIEC, 'Annual Report 2014' (26 March 2015) 21 <https://www.ffiec.gov/PDF/annrpt14.pdf> accessed 2 August 2018.
[36] FRS Enhanced Cyber Risk Management Standards, 10.
[37] FFIEC, 'FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors' (June 2015) <ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf> accessed 18 August 2018.

determine their criticality for the sector and the exchange of intelligence between relevant financial sector agencies within and outside the US.[38]

Due to evolving cyber threats and attacks requiring thorough and long-term trend analysis of attack specificities, the Financial Systemic Analysis and Resilience Center (FSARC) was created by a consortium of 8 leading US banks with the objective of enhancing cyber resilience within the financial sector and improve intelligence. The FSARC operates under the FS-ISAC to "identify and prioritise the most persistent systemic operational risks to the US financial sector" through collaboration with the stakeholders, industry and government partners.[39] This indicates the sector's commitment towards taking collective action against cyber threats, attacks and vulnerabilities. However, Mohan et al note a major limitation to the FSARC's activities in integrating operations beyond the US to other jurisdictions, where collaboration is required with intelligence agencies in other jurisdictions to address the multifaceted and international nature of systemic risks.[40]

This section has provided an overview of relevant institutions in the US financial regulatory landscape. Here, we note an entirely different approach from the UK in terms of structure, although sharing a few similar objectives. While financial regulation in the UK is clearly undertaken by the BOE, FCA and PRA, the US approach appears overwhelming due to the multiplicity of regulators and objectives, a problem that has been highlighted in several reports[41]. In particular, duplication of responsibilities is observed across many authorities proposing best practice rules for effective cybersecurity governance and management, and this may be argued to inhibit effective regulation, communication and cooperation. A major reason behind this challenge as is been argued, has been found in the distribution of

[38] G.A. Garrett, *Cybersecurity in the Digital Age: Tools, Techniques, & Best Practices* (Wolters Kluwer Law & Business 2018) 254.
[39] Financial Systemic Analysis and Resilience Center, 'US Treasuries (UST) Initiative Highlights Treasury Market Practices Group' (23 October 2018) 3 <https://www.newyorkfed.org/medialibrary/Microsites/tmpg/files/FSARC_TMPG_Presentation.pdf> accessed 23 July 2020.
[40] R. Ellis and V. Mohan, *Rewired: Cybersecurity Governance* (Wiley 2019) para 6.6.2.
[41] US Government Accountability Office (US GAO), 'Financial regulation: Complex and Fragmented Structure Could Be Streamlined to Improve Effectiveness' GAO-16-175 (25 February 2016) 2 <https://www.gao.gov/assets/680/675400.pdf> and The Volcker Alliance, 'Reshaping the Financial Regulatory System: Long delayed, now crucial' (2015) <www.volckeralliance.org/sites/default/files/Reshaping%20the%20Financial%20Regulatory%20System%20-%20The%20Volcker%20Alliance.pdf> accessed 23 July 2020.

regulatory responsibility based on business operations e.g., banking and securities,[42] as opposed to the UK where distribution of responsibility is based on objectives i.e., conduct and prudential regulation. The next section discusses cyber risks and crimes regulated by the institutions and intends to employ a narrow categorisation based on analysis employed in Chapter 2.

5.3 Emerging Risk in the US Financial Sector

Prevalent Cybercrimes in the US Financial Sector

Examples of cyber occurrences in the sector include the target on American FIs by Russian and Ukrainian attackers for a period of seven years which involved access to over 160 million credit and debit card information resulting in a loss of about $300 million.[43] Another example of a data breach was the 2014 cyberattack on JP Morgan Chase which involved a DDoS attack and data theft affecting over 83 million account information. The stolen information was then used in laundering money and carrying out wire fraud schemes which yielded about $100 million. The cost of a DDoS attack on FIs can be particularly damaging as the attack disrupts networks, services and other infrastructure with the average cost of a one-minute downtime estimated at $22,000[44].

Similarly, in 2016, the SEC's computer system was hacked as a result of a software vulnerability. The hackers gained access to private information which were believed to provide a possible basis to carry out insider trading.[45] Such an attack to a major financial industry regulator and unauthorised access to critical information could significantly undermine public trust in the financial system. Indeed, it is impossible for a house owner to trust a watchman with his safety if the watchman fails to possess the necessary tools for securing his own safety against thieves. Nevertheless, the SEC further notes in its statement

[42] The Volcker Alliance, 'Reshaping the Financial Regulatory System' 14.
[43] M. Kurosu, *Human-Computer Interaction. Interaction Contexts: 19th International Conference, HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings* (Springer International Publishing 2017) 540.
[44] Ponemon Institute LLC, 'Cyber Security on the Offense: A Study of IT Security Experts' (November 2012) 1 http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf > accessed 10 September 2019.
[45] SEC, 'Statement on Cybersecurity' (20 September 2017) <https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20> accessed 12 September 2019.

the increasing rate of cyberattacks and the need for managing such risks through resilience and recovery.

An even recent breach was the Capital One Financial Corp case where a hacker through the bank's network, gained access to data of about 106 million credit card applications, containing financial/sensitive data, resulting in a current cost of about $150 million for the bank to rectify the breach.[46]

In a bid to minimise such cyber risk in the supply chain process, FIs such as Bank of America, JPMorgan Chase, BNY Mellon, Wells Fargo, and American Express have created TruSight, a company which will help to set best practice standards for the comprehensive assessment and control of third party risks.[47] This is due apparently to an increase in the data and IT risks posed by third parties, particularly in relation to data breaches. Indeed, third-party outsourcing arrangements are a major source of data breaches. Such arrangements may give rise to service quality risks, security risks, reputational risks, and associated regulatory costs for non-compliance. To minimise these risks, banks may implement FFIEC due diligence recommendations for appointing a third-party service provider. Some key relevant components include: (i) qualification, background and policy of the provider; (ii) capability to deliver services effectively; (iii) internal control processes and security incidents; (iv) adherence to laws and regulation and (v) incident recovery and business continuity.[48]

Scale and Impact of Cybercrime

The impact of cybercrimes can only be estimated where there is accurate and timely reporting of incidents. In the absence of this, prosecution of cyber criminals as well as developing techniques to respond and defend against these attacks become almost impossible. The Internet Crime Complaint Center (IC3), previously known as the Internet Fraud Complaint Center (IFCC) was established in May 2000, through a coordination between the Federal

[46] Office of Financial Research (OFR), 'Annual Report to Congress' (2019) 39 <https://www.financialresearch.gov/annual-reports/files/OFR-Annual-Report-2019.pdf> accessed 15 July 2020.
[47] TruSight, 'The New Industry Standard for Third-Party Risk Fact Sheet' <https://s3.us-east-1.amazonaws.com/trusightsolutions-com/documents/third-party-risk-assessment-fact-sheet-trusight-solutions.pdf?mtime=20190911161426> accessed 12 September 2019.
[48] FFIEC IT Examination Handbook: Outsourcing Technology Services.

Bureau of Investigation (FBI), the Bureau of Justice Assistance (BJA) and the National White Collar Crime Center (NW3C) with the aim of tackling emerging online fraud issues.[49]

Similar to the UK Action Fraud,[50] the IC3 is the body designated by the US government in charge of fraud and cybercrime reporting. The IC3 platform consists of mainly data from victim report. Although, the FFIEC suggests the IC3 may be used as a response/reporting resource for financial institutions.[51] The establishment of each of these bodies for reporting is useful in terms of having a central system for reporting. However, the major issue which remains is whether such a system will be effective due to the involvement of multiple agencies in fraud investigation and different systems for dissemination of information. Indeed, Rorie observes that the provision of multiple approaches for dealing with such breaches in regulatory agencies pose serious challenges in measuring the impact of the crime.[52]

The IC3 publishes an annual report which shows the extent of cybercrime as well as steps taken by the center and law enforcement to address it. According to its 2019 report, complaints received were estimated at 467,361 a 32.8% increase from the previous year, with the most common complaints being personal data breach, non-payment/non-delivery fraud and phishing.[53] Meanwhile, the total losses from complaints also increased by 29.63%, estimated at $3.5 billion.[54] In the same year, figures published by the IC3 indicate a significant increase in the cost of internet crimes when compared with data reported in the previous years' 2016[55], 2017[56] and 2018.[57] The report estimates losses from frauds,[58] scams[59] and data breach[60], some of which may pertain to financial institutions. The IC3 provides useful tools for combatting cybercrimes and operates by creating a primary network for

[49] Sandra K Hoffman and Tracy G McGinley, *Identity theft: a reference handbook* (ABC-CLIO 2010) 130.
[50] The centre designated by the UK government in charge of fraud and cybercrime reporting.
[51] FFIEC, 'Cybersecurity Resource Guide' 7.
[52] M.L. Rorie and C.F. Wellford, *The Handbook of White-Collar Crime* (Wiley 2019) 40.
[53] Internet Crime Complaint Center (IC3), '2019 Internet Crime Report' 3 <https://pdf.ic3.gov/2019_IC3Report.pdf> accessed 6 September 2019.
[54] ibid.
[55] IC3, '2016 Internet Crime Report' <https://pdf.ic3.gov/2016_IC3Report.pdf > accessed 6 September 2019.
[56] IC3, '2017 Internet Crime Report' <https://pdf.ic3.gov/2017_IC3Report.pdf> accessed 6 September 2019.
[57] IC3, '2018 Internet Crime Report' <https://pdf.ic3.gov/2018_IC3Report.pdf> accessed 6 September 2019.
[58] This covers identity theft, credit card fraud, ransomware, denial of service attacks and phishing/vishing/smishing.
[59] This covers business email/email account compromise scams.
[60] This covers corporate data breach.

notifying the public on internet crimes, collaborating with the private sector, government and international agencies, as well as providing a remote database for law enforcement to access relevant information and resources for investigating cybercrime cases.

Unlike the UK Finance *Fraud the Facts* report, there is not a single report which presents a comprehensive detail on relevant e-banking crimes and losses in the US financial sector. The 2018 Federal Reserve Payments Study by the FRS, however, reports the total remote (card-not-present) fraud value by card payment type. This is presented in the graph below.[61]

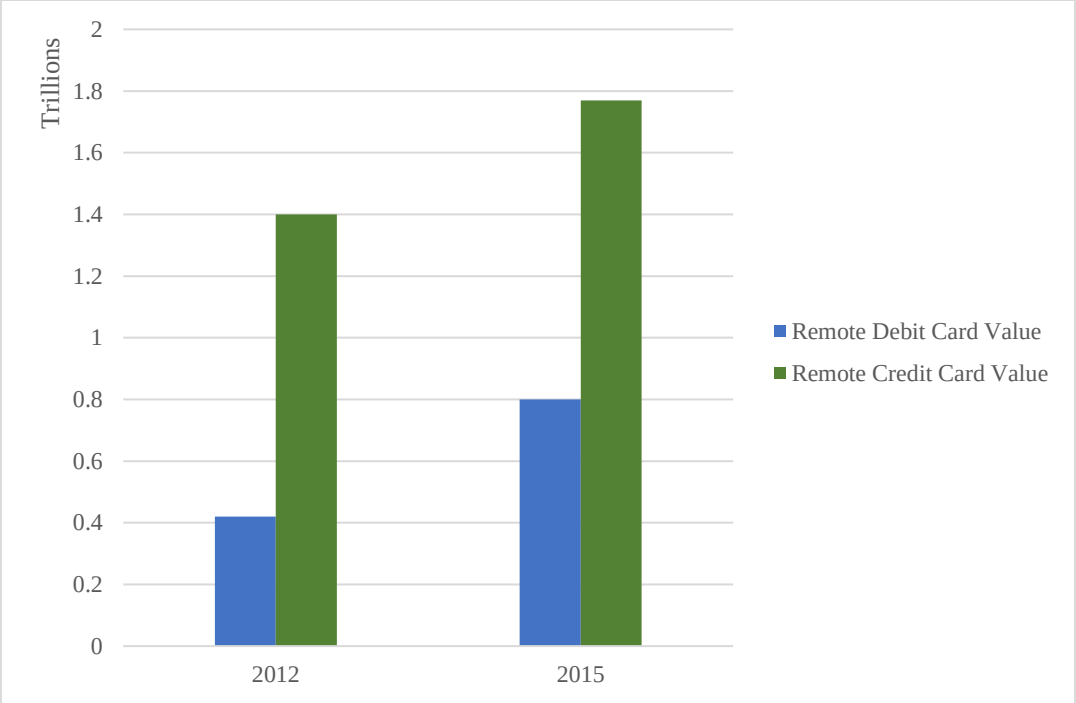

Figure 5-2 *Remote card payments fraud value by payment type in the US, 2012 and 2015*

While this study fails to show a clear picture of the current threat landscape, it does show increasing losses due to remote banking fraud. Consistent with reports of increasing unauthorised remote banking fraud in the UK, remote debit and credit card payments fraud

[61] Data gathered by the Depository and Financial Payments Survey (DFIPS) and reported in FRS 'Changes in U.S. Payments Fraud from 2012 to 2016: Evidence from the Federal Reserve Payments Study' (October 2018) 39 <https://www.federalreserve.gov/publications/files/changes-in-us-payments-fraud-from-2012-to-2016-20181016.pdf> accessed 6 July 2020.

rose by 90.48% and 26.43% between years 2012 and 2015, respectively. These figures may also suggest a higher fraud risk in the US financial services sector with loss values amounting to more than ten times the total fraud value of unauthorised remote banking fraud in the UK (**Figure 4-2**). Although, values provided by the two are only comparable to a small extent as they are each representative of different market sizes.

Moreover, limitations exists, in that analysis and conclusions are drawn from a small and outdated data set. It is therefore proposed that the US financial sector publishes its annual fraud statistics, which it gathers. These statistics as can be seen in the UK provide not only details on losses, but also recommendations by the sector in its attempts to tackle each type of fraud as well as yearly implementation reviews/successes.

5.4 The Self-Regulatory Fundamentals

Reflexivity in Organisational Requirements of US Financial Institutions

This *section* follows a *similar approach* to that of the *previous chapter* by exploring annual reports to examine the various stages of risk management followed in each bank. Due to the limited amount of information contained in the annual reports, related publications including statements and insights were carefully selected to ensure thorough analysis. It is to be noted that results from the studies do not reflect the wider industry and may not be generalisable beyond the banks studied. However, it is specifically intended to explore self-regulatory approaches in US banks rather than to draw general conclusions which may have been possible if more institutions were included in the dataset.

JPMorgan Chase (Chase) spends about $600 million annually on cybersecurity and employs over 3,000 employees to achieve its mission of protection of consumer privacy and cyber safety.[62] This indicates the amount of money spent by large organisations in implementing their security policies and strengthening the resilience of their systems. Common cyber risks highlighted in the *Chase Annual Report 2019* include unauthorised access to confidential data, data disruption or destruction, denial of service attacks, third party

[62] JPMorgan Chase (Chase), 'Annual Report 2018' 35 <https://www.jpmorganchase.com/corporate/investor-relations/document/annualreport-2018.pdf> accessed 1 October 2019.

failures, breach or data compromise and clients' weak security systems and processes.[63] To manage its cybersecurity risks, the bank adopts the following measures:

Risk Assessment Processes	Simulation exercises to test and assess resilience of its systems.[64] This is useful for evaluating the physical capabilities of systems to respond to a threat/an attack. Use of machine learning[65] for proactive monitoring.[66]
Risks Identified to Business Operations	Operational risks and risks to its resilience resulting from cyber incidents, such as third-party outsourcing risks which could cover anything from service failure to data compromise and customer risks by failing to ensure security of their systems and transactions.[67]
Risk Control Frameworks	A cybersecurity program for the prevention, detection and response to cyber incidents and a Cybersecurity and Technology Control Unit (CTCU) in charge of governing and supervising the program. A cybersecurity Incident Response Plan (IRP), also covering coordination with law enforcement and government authorities.[68] A Third-Party Oversight framework for managing contractual dealings. An Independent Risk Management (IRM) function for overseeing operations of the cybersecurity programme and the CTCU. A Security Awareness program covering staff training to supplement the bank's IT risk and cybersecurity management policies, ethics and performance.[69]
Risk Review	A submission of at least a yearly report by the Global Chief Information Officer, Chief Information Security Officer (CISO) and Chief Technology

[63] Chase, 'Annual Report 2019' 130 <https://www.jpmorganchase.com/corporate/investor-relations/document/annualreport-2019.pdf> accessed 1 July 2020.
[64] Chase, 'Understanding Our Climate-Related Risks and Opportunities' (May 2019) 7 <www.jpmorganchase.com/corporate/Corporate-Responsibility/document/jpmc-cr-climate-report-2019.pdf> accessed 6 July 2020.
[65] Machine learning may refer to the use of algorithms for detecting patterns, regularities, and even irregularities which can be shape predictions in risk management decisions.
[66] Chase, '2019 Proxy Statement' (6 April 2020) 68 <https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/proxy-statement2020.pdf> accessed 6 July 2020.
[67] Chase, 'Annual Report 2019' 130.
[68] ibid.
[69] Chase, 'Annual Report 2019' 131.

	Control Officer to the Board's Audit Committee regarding the bank's cybersecurity program, proposed updates, security guidelines and performance, and key cybersecurity incidents.[70] Conducts quarterly phishing tests as part of its periodic testing measures. Monitors customer activities to periodically assess behavioural patterns to identify and prevent evolving schemes implemented adopted by fraudsters.[71]

Table 5-1 *Risk management frameworks adopted by Chase*

In its 2019 Annual Report, the Bank of America (BofA) faces several risk factors including a breakdown or breach of its systems/infrastructure or those of its outsourcing arrangements, cyberattacks and the financial circumstance and consequences of its services due to the prearranged exit of the UK from the European Union.[72] Similar to Chase, its key operational risks include cybersecurity as it notes that such risks may affect the confidentiality, availability or integrity of its systems, including those of its service providers, resulting in financial, reputational and legal consequences.[73] In addressing such risks and minimising their impact, the bank adopts the following measures:[74]

Risk Assessment Processes	An independent testing overseen by the IRM and performed by the Enterprise Independent Testing unit. Scenario-based testing and exercise which simulates cyberattacks for detecting system vulnerabilities.[75]
Risks Identified to Business Operations	Cybersecurity risks resulting from service disruptions, operational failures, security breach, malware attacks affecting the confidentiality, availability and integrity of data, services and systems of the bank and third parties.

[70] Chase, '2019 Proxy Statement' 57.
[71] Chase, 'Annual Report 2019' 131.
[72] Bank of America Corporation (BofA), 'Annual Report 2019' 43 <http://investor.bankofamerica.com/annual-reports-proxy-statements/2019_Annual_Report> accessed 18 July 2020.
[73] ibid 98.
[74] BofA, 'Annual Report 2019' 98.
[75] BofA, 'Cyber security: Insights from Bank of America's chief information security officer' (October 2019) <https://workplaceinsights.bofa.com/articles/2019/10/froelich.html> accessed 18 July 2020 (BofA, Cyber security Insights 2019).

Risk Control Frameworks	Internal policies containing a detailed information security programme established to safeguard the bank by facilitating measures to detect, prevent and manage relevant risks. The implementation of the information security program is managed by the Global Information Security Team. Implements thorough quality assurance measures to detect issues and risks from third-party dependencies and its operations so as to eliminate gaps and vulnerabilities. The Board and the Enterprise Risk Committee (ERC) are to provide IT security risk governance, with the Board also overseeing how its significant risks including cyber risks are being identified, measured, supervised and managed.[76] Coordination with industry stakeholders to share and gather intelligence.[77]
Risk Review	The Board and ERC regularly review IT and cybersecurity risks report and take presentations during the course of the year on IT and cybersecurity issues.[78] The ERC is also responsible for the annual review of the bank's Global Information Security program, policies, technical and physical capabilities, in compliance with laws and industry guidelines.[79] Regular cybersecurity exercises aimed at enhancing capabilities.[80]

***Table 5-2** Risk management frameworks adopted by BofA*

Findings from this study are consistent with the UK reports showing that third-party risks are of growing concern to financial institutions. Both studies note the importance of independent oversight of cyber risk management, a function that has been observed to influence risk

[76] BofA, 'Proxy Statement' (9 March 2020) 17 <http://investor.bankofamerica.com/static-files/599c40f7-721e-47fd-8fe1-a63a89d47532> accessed 5 July 2020.
[77] ibid 26.
[78] BofA, '2020 Proxy Statement' 25.
[79] ibid 26.
[80] BofA, Cyber security Insights 2019.

management policies,[81] ensure robust risk governance[82] and limit risk exposures[83]. They also indicate the attentiveness to the FRS's proposal in the Enhanced Cyber Risk Management Standards report for placing cybersecurity within the IRM function. Meanwhile, the use of simulation exercises in both studies show ways by which institutions engage in self-learning of vulnerabilities and risks in their security frameworks to develop adequate responses.

The result from these studies also provide some support for the argument advocated in Chapter 3 on placing cybersecurity duties on directors to ensure liability in the event of non-compliance. Besides, the involvement of a CIO in a senior management position has been found to considerably influence the effectiveness of the security and risk management framework.[84] While both studies suggest the importance of board awareness of the cybersecurity programme, the report from BofA shows the active involvement of the Board at several stages of the process. This in line with regulatory guidance that effective cybersecurity frameworks involves a top-down approach where senior management collaborates with staff to "understand, prioritize, communicate, and mitigate cybersecurity risks".[85]

In addition, studies indicate stakeholder collaboration as essential for the management of cybersecurity risks. Collaborative learning is key in financial sector reflexive governance as it provides FIs with knowledge on the risk landscape which can be used for enhancing the design and architecture of their information security systems.

Both studies not only reinforce the need for effectiveness of cybersecurity regulatory frameworks, but also show banks efforts to bolster cyber defences. Although beyond the scope of this research, they also suggest significant regulatory implications for institutions based on the regulatory uncertainties surrounding the Brexit transition period in

[81] Georges Dionne, Olfa Maalaoui Chun and Thouraya Triki, 'The governance of risk management: The importance of directors' independence and financial knowledge' (2019) 22 Risk Management and Insurance Review 247, 249.
[82] Alessandra Mongiardino and Christian Plath, 'Risk governance at large banks: Have any lessons been learned?' (2010) 3 Journal of Risk Management in Financial Institutions 116, 117.
[83] Andrew Ellul and Vijay Yerramilli, 'Stronger risk controls, lower risk: Evidence from US bank holding companies' (2013) 68 The Journal of Finance 1757, 1796.
[84] Cecilia Qian Feng and Tawei Wang, 'Does CIO risk appetite matter? Evidence from information security breach incidents' (2019) 32 International Journal of Accounting Information Systems 59, 60.
[85] OCC, SEC, 'Cybersecurity and Resiliency Observations' (27 January 2020) 2 <http://sec.gov/files/OCIE-Cybersecurity-and-Resiliency-Observations-2020-508.pdf> accessed 11 January 2021.

which EU regulations applicable to US banks in the UK may be amended or substituted with UK regulations.

5.5 Reflexivity in Regulation and Supervision

The section summarises some cybersecurity guidelines associated with reflexivity, issued by relevant financial regulators in the US overtime and discusses major themes relating to cybersecurity regulation and supervision in the sector. In particular, it outlines roles and responsibilities of FIs relating to the security of customer data, cyber incident disclosure, security of networks, systems and processes. Notice that in the following table, terms associated with reflexivity, explored also in Chapter 4 are highlighted in italics.

Regulator	Guidelines
FRS	• The 2003 Interagency Paper "Sound Practices to Strengthen the Resilience of the U.S. Financial System" for developing necessary response capabilities for efficient recovery and restoration of system operations activities in financial markets. In particular, *routine tests of response and recovery plans*.[86]
OCC	• The 2003 Third-Party Relationships Risk Management Guidance involving a "*continuous life cycle*" where FIs assess the third party's resilience frameworks based on their response to cyber threats/attacks, clear business continuity and disaster recovery processes.[87]
FDIC	• Interagency Guidelines Establishing Information Security Standards under Appendix B to Part 364 of its 2000 - Rules and Regulations. This covers: *a disclosure by FIs* to regulators and law enforcement agencies on procedures put in place for responding in situations of unauthorised access to information systems, and *regularly testing* of essential

[86] OCC, 'Interagency White Paper on Sound Practices to Strengthen the Resilience of the US Financial System' (11 April 2003) 17813 <https://www.occ.treas.gov/news-issuances/bulletins/2003/OCC2003-14a.pdf> accessed 15 August 2019.
[87] OCC, 'OCC Bulletin 2013-29| Third-Party Relationships: Risk Management Guidance' (30 October 2013) <https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html> accessed 8 October 2019.

	controls, systems, and processes in its information security programme as part of the risk assessment plan.[88]
SEC	• Rule 30 of Regulation S-P, which provides that SEC regulated financial institutions are to implement necessary policies and procedures towards safeguarding the confidentiality of customer data, including *safeguard against any predicted threats or risks* to the 'security or integrity'.[89] • Division of Corporation Finance's Disclosure Guidance Topic No. 2 on *disclosure obligations of potential cyber risks that arise in the course of business* such as data compromise, unauthorised access to information systems etc.[90]
CFPB	• 9 Data Protection Principles governing access, transmission, consent, data authorisation, security, Transparency, accuracy, dispute resolution and accountability to guide stakeholders on the use of customer data. Rule 5 states that FIs are to ensure that cyber*security procedures adapt effectively to evolving risks*. [91]
FFIEC	• The Uniform Rating System for Information Technology (URSIT).[92] The URSIT is used by federal and state regulators to *assess* information security risks and risk management employed by financial institutions, service providers and associates in order to *determine* institutions which require *regulatory or supervisory intervention* to ensure effective risk management.[93] Supervisory intervention is designated according to the rating. • FFIEC IT Handbook 2003, Appendix (A) on IT Examination procedures provides for the *assessment of previous records for unresolved IT*

[88] FDIC, '2000 – Rules and Regulations' Rule C - 1(g) and C - 3.
[89] 17 C.F.R. 248.30.
[90] SEC, 'CF Disclosure Guidance: Topic No. 2' (13 October 2011) <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm> accessed 16 August 2018.
[91] CFPB, 'Consumer Data Protection Principles' (2017) <https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf> accessed 10 July 2020.
[92] The US first supervisory framework for cyber security practices at FIs published in 1978. Revised in (January 20, 1999), *see* 64 F.R. 3109.
[93] FFIEC, 'Uniform Rating System for Information Technology' (19 October 2016) 9 <https://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers/risk-based-supervision/uniform-rating-system-for-information-technology.aspx#:~:text=The%20Agencies%20use%20the%20Uniform,financial%20institutions%20and%20their%20TSPs.&text=The%20URSIT%20is%20based%20on,Acquisition%2C%20and%20Support%20and%20Delivery.> accessed 15 July 2020.

	incidents or problems, assessment of response to such problems and *identification of IT or operational changes* that may heighten security risks.[94]

Table 5-3 *Regulatory Guidelines Associated with Reflexivity in the US*

Cyber Incident Communications and Reporting

FIs are under an obligation to notify both customers and regulators of cyber incidents at both federal[95] and state level[96]. In the US, federal law enforcement agencies such as the FBI IC3, Homeland Security and the National Cyber Investigative Joint Task Force are authorised to receive cyber incident and breach notifications from private sector entities, including financial institutions.[97] This is important as information disclosed assist with providing relevant information to regulators and law enforcement for effective conduct monitoring, investigation and enforcement.[98] As seen in ***Table 5-3*** above, the FFIEC's Examination guidelines appears to indicate the availability and accessibility of records of IT incidents, which can only be useful where there has been accuracy in reporting. Meanwhile, a consideration of previous records with associated responses and existing changes for possible/future risks characterize reflexive practices, involving a combination of retrospective and forward-looking processes towards developing well-informed security frameworks.

FIs may also report cyber-related incidents using Suspicious Activity Reports containing the impact, timing, location and characteristics of the incident.[99] Meanwhile, platforms in which FIs may share and exchange cyber threat intelligence and indicators

[94] FFIEC, IT Examination Handbook, Appendix A: Examination Procedures.
[95] FRS, 'Interagency Guidance for response programs for unauthorised access to customer information and notice' (1 December 2005) 15 <https://www.federalreserve.gov/boarddocs/srletters/2005/SR0523.htm> accessed: 20 September 2019 (FRS Interagency Guidance for response programs for unauthorised access).
[96] 23 NYCRR 500, Section 500.17.
[97] Federal Bureau of Investigation (FBI), 'Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government' <https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view> accessed 10 July 2020.
[98] CRS, 'Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework' (Updated 10 March 2020) 5 <https://fas.org/sgp/crs/misc/R44918.pdf> accessed 10 July 2020.
[99] Financial Crimes Enforcement Network (FinCen), 'Advisory to FIs on Cyber-Events and Cyber-Enabled Crime FIN-2016-A005' (25 October 2016) 7 <https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf> accessed 10 July 2020.

include the DHS Automated Information Sharing Program, FS-ISAC, InfraGard, Financial and Electronic Crimes Task Force.[100]

Conducting Simulation Tests and Exercises

As part of its cybersecurity functions, some regulators offer video simulation exercises to financial institution to improve discussions of the cyber risk landscape and techniques for mitigating against these risks.[101] Likewise, the FS-ISAC in partnership with the financial services sector may conduct a number of exercises, drills and simulation exercises[102] to test sector resilience and enhance coordination.[103] Such simulation exercises are reflexive practices in that through the analysis of predicted real life cyber threat scenarios, knowledge is produced from participant responses and then reproduced, by way of changes implemented towards developing response capabilities. As such, when designing these exercises, sometimes used interchangeably with terms such as 'tests' and 'examinations', FIs must take into account regulatory guidelines such as those in ***Table 5-3*** requiring tests which are continuous, routine and regular.

Outsourcing Arrangements

According to the FRS, FIs must "test the service provider' s business continuity and contingency plans on a *periodic* basis to ensure adequacy and effectiveness".[104] Likewise, in the FFIEC Handbook, FIs and outsourcing providers are advised to examine scenarios likely to cause major interruptions to their services, evaluate their response capabilities, identify very conceivable recovery measures and update business continuity plans to address key service recovery.[105] Like the FRS which note the importance of periodic testing, the Handbook also notes ongoing monitoring[106], similar to the OCC's requirement of a *continuous life cycle* for third-party risk management processes as seen in ***Table 5-3***, to ensure

[100] *See* FFIEC Cybersecurity Resource Guide.
[101] Federal Deposit Insurance Corporation, 'A Framework for Cybersecurity' (2015) 8.
[102] E.g., Cyberattack Against Payment Systems (CAPS) Exercise.
[103] Financial Services Information Sharing and Analysis Center (FS-ISAC), 'Exercises' <https://www.fsisac.com/hubfs/Resources/FS-ISAC_ExercisesOverview.pdf> accessed 10 July 2020.
[104] FRS, 'Guidance on Managing Outsourcing Risk' (5 December 2013) 11 <https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf> accessed 15 July 2020.
[105] FFIEC IT Examination Handbook, Appendix J-7 Strengthening the Resilience of Outsourced Technology Services.
[106] ibid Appendix J-4.

resilience of outsourced services. All of which, in effect, represent an important feature of reflexive governance for drawing on, adjusting and replicating activities based on monitoring results.

While proposed guidelines/requirements may be effective in closing some gaps in cybersecurity risk management, it has however been suggested their voluntary nature, particularly in incident reporting, may hinder effectiveness.[107] In this regard, US financial regulators have recently proposed rules requiring notification of a cyber incident by FIs to agencies. Under these rules, FIs are under a 36-hour deadline to report any 'computer-security incident' that escalates to a 'notification incident' to their primary federal regulator as soon as possible, following the FIs belief "in good faith" of the occurrence. Of importance, the proposed rules define a notification incident as a computer-security incident that an FI in good faith, considers as having the potential to cause a material disruption, degradation, or impairment i.e. to the ability of the FI to conduct its operations, activities, or processes, or in its product and service fulfilment to a significant number of its customers, "in the ordinary course of business; any business units of a banking organization, including associated operations, services, functions and support, and would result in a material loss of revenue, profit, or franchise value; or those operations of a banking organization, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States."[108]

Despite the 36-hour deadline, regulators note possible difficulties for FIs in establishing whether an incident satisfies the notification incident requirement upon awareness of the incident, especially where it occurs outside typical business hours, highlighting that FIs may require a "reasonable amount of time" in making such judgements.[109] While the considerations are valid, it is argued that such suggestions of a reasonable amount of time may be relative, and thus yield unfavourable outcomes. On the

[107] Kristin N Johnson, 'Innovating to new heists: regulating cyber threats in the financial services industry' (2017) The Most Important Concepts in Finance 28, 50.
[108] FDIC, 'Proposed Rules: Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers' Vol. 86, No. 7 (*Federal Register*, 12 January 2021) 2302 <https://www.fdic.gov/news/board/2020/2020-12-15-notice-sum-c-fr.pdf> accessed 15 January 2021 (Joint Proposed Computer-Security Incident Notification Rules).
[109] ibid 2302.

other hand, this requirement appears to mirror the regulatory thought process behind the NIS Regulations 2018, as recognition of the need for a "reasonable amount of time" prior to incident notification, may result in a late notification of the incident, depending on the assessment required. With this in mind, the UK financial sector needs to revisit its current frameworks in light of the NIS Regulations 2018 which appear to better serve its cybersecurity objectives. In the same fashion, it may benefit the US to set additional benchmarks in terms of the "reasonable amount of time" standard, requiring FIs to provide reasons, where the regulator, taking into account the incident notification requirement finds there to have been an unreasonable delay and where it finds that notification exceeds the 36-hour deadline. Equally, a notification requirement to affected customers, should also be considered.

In addition to contractual incident reporting provisions between FIs and service providers, the US regulators also propose a bank service provider notification requirement which will be enforced directly against service providers, where the provider fails to comply with the requirement to notify two or more individuals in the affected FI.[110] In contrast, the UK currently has no such requirements or proposals under review for creating a specific cyber incident obligation for service providers, except for current provisions of the DPA 2018 which impose liability on service providers for data breaches due to non-compliance with the law or against lawful instructions from the controller i.e. FIs. Hence, an adoption and implementation of the service provider notification requirement, would not only minimise prolonged impact or costs for business operations, but also facilitate prompt reporting to regulators, while ensuring accountability of service providers for the security of services provided.

5.6 The 'Regulatory Co-Existence' Hypothesis

This section will further reinforce the arguments presented in Chapter 3 on regulatory co-existence and offer a vital context against which we can test our hypothesis and understanding of how the sector is effectively self-regulated against a backdrop of state regulation.

[110] ibid 2303.

Civil Fines and Penalties: Sanctioning Regimes

Apart from the regulatory responses to cybercrimes, the US addresses cybercrime through law enforcement through the engagement of various government agencies and departments such as the FBI's Cyber Division which collaborates with regional, national and international law enforcement agencies to combine efforts and resources against cyberattacks.

In the US, law enforcement has been quite successful in enforcing cybercrime charges. FIs have also faced numerous remedial, litigation and regulatory costs as a result of cybersecurity breaches, particularly relating to cyber risk detection, notification and response.[111] As an example of a successful enforcement, in July 2019, the Federal Trade Commission (FTC)[112] and CFPB after a coordinated investigation, concluded a settlement fine with Equifax encompassing compensation/remedies for affected customers and states due to its 2017 data breach.[113]

Cyber Incident Examples	Relevant Cybersecurity Laws and Regulations	Regulatory Costs and Penalties
• Failure to implement a timely response to identified vulnerabilities. An incomprehensive and inaccurate IT documentation. Reactive system patching policies. No regular audits. Equifax 2017[114]	GLBA 1999 requiring the compliance with disclosure provisions relating to sensitive data, physical, and technological security of customer data.[115]	Joint fine by the CFPB and FTC of $575 million.

[111] Latham and Watkins LLP, 'Cybersecurity regulation and best practice in the US and UK' <https://www.lw.com/thoughtLeadership/Cybersecurity-regulation-and-best-practice> accessed 16 August 2018.
[112] The FTC is an independent organisation in the US with civil U.S. antitrust law and the consumer protection enhancement objectives.
[113] FTC, 'Equifax to pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach' (*News Release*, 22 July 2019) <ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related> accessed 6 September 2019.
[114] US Senate Equifax Report, 23 - 31. Other applicable Laws include the Fair Credit Reporting Act 15 U.S.C. 1681 and the Dodd-Frank Act 12 U.S.C. 5492(a).
[115] 15 U.S.C. 6801(b).

• Hacking involving the theft of personal sensitive information such as names, e-mail, addresses and phone numbers of 83 million customers. JP Morgan Chase 2014[116]	Not applicable as no report on investigation.	Not applicable.
• Exploitation of bank's website vulnerabilities resulting in the theft of over 360,000 card details of its customers. Citibank Data Theft 2011[117]	GLBA (15 U.S.C. 6801). California Civil Code 1798.82 requiring data breach notification to customers without undue delay. California Online Privacy Protection Act 2003, 22575 - 22578 setting out instances where an operator may be in violation of a privacy policy.	$420,000 encompassing civil penalties, investigation, and prosecution costs.[118]

Table 5-4 *Examples of US Financial Sector Cybersecurity Sanctions*

As pointed out in Chapter 3, reflexivity acknowledges the constraints of learning, and it is only through appropriate enforcement regimes that the *preserving effect* outlined by Beck may be achieved.

The CFPB has enforcement and supervisory authority over Equifax pursuant to the Dodd-Frank Act, whereas the FTC does not have the supervisory authority to assess compliance with its Act[119]; and would usually rely on the exercise of its enforcement authority post-incident.[120] Amongst other things, the CFPB in deciding whether to initiate an

[116] OECD, *Enhancing the Role of Insurance in Cyber Risk Management* (OECD Publishing 2017) 31.
[117] CEIP, Timeline of Cyber Incidents Involving Financial Institutions (2020).
[118] Office of the Attorney General (OAG), 'Citibank Final Judgement' <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/citibank_final_judgement.pdf?> accessed 14 July 2020.
[119] 15 U.S.C. 45(a).
[120] US GAO, 'Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach' (August 2018) 7 <https://www.gao.gov/assets/700/694158.pdfa> accessed 14 July 2020.

enforcement proceeding, takes into account a number of mitigating factors including the gravity of the violation, the degree and scope of the violation, the number of violations, the possible recurrence of the violation, previous regulatory proceedings, cooperation and awareness of the violation. The FTC, on the other hand, considers factors such as the alignment of the institution's information security procedures with its size.

Violation-specific factors used by the CFPB, and the institution-process factor used by the FTC does reveal considerations of proportionality and fairness. However, questions arise as to the metric used in the determination of these factors. Moreover, compared to the UK's FCA which is guided by well-defined principles of punishment in deciding its penalties, the CFPB provides hardly any explanation as to how it makes penalty decisions.[121] Meanwhile, the Equifax hack does uncover reactive regulation and weaknesses in monitoring and supervision by regulators, as they failed to take precautions until Equifax's vulnerabilities were exposed. If Equifax's conduct was regularly checked/monitored, it will eliminate reduced accountability and feigned compliance, thus in favour of the co-existence hypothesis.

Following the Rational Actor Model in Chapter 3, the issuance of public notices and reports by regulators form part of adequate sanctions for imposing liability. Although, under the model Equifax could have been sanctioned for all of the profits it made during the breach. Meanwhile, under the Organisational Process Model, liability could have been imposed on the units, in this case, the IT unit, whose role was to ensure that standard operating procedures like patching were up to date.

The adoption of a Personal Data and Privacy Act has been long deliberated in the US since the Citigroup Data theft. In the Citibank case, the state of California amongst other states affected, initiated enforcement proceedings against it for the compromises of over 80,000 citizens as part of the breach.[122] The state sought to enforce relevant laws as the bank failed to comply with its own privacy policies and was aware of the vulnerabilities but failed to take reasonable steps to permanently repair them. While this set a good example for data breach regulation in the US, it was not followed in the JPMorgan Chase case as up until date,

[121] Eric Mogilnicki, 'CFPB has too much flexibility in assessing fines' (16 April 2019) <www.americanbanker.com/opinion/cfpb-has-too-much-flexibility-in-assessing-fines> accessed 2 August 2020.
[122] OAG, 'Citibank Complaint' <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/citibank_complaint.pdf?> accessed 14 July 2020.

there was no information relating to fines or penalties imposed on the bank for the breach.[123] As at that time, the bank was reported to have placed the onus on customers for the detection and reporting of fraudulent transactions.[124] While it is reasonably expected that customers reported and took note of any suspicious activities on their account, detection appears to be a more technical duty best left to the bank.

Cybersecurity breaches are fundamentally different from other crimes in the financial markets and a possible consideration for regulators in the US where there is no federal data breach notification provision is to introduce it as a mitigating factor in the determination of penalties and enforcement, having regard to timing and materiality. Thus, echoing Majone's argument for substituting laws by incentives.[125]

Public-Private Partnerships in Law Enforcement

The financial services sector cannot on its own tackle the growing threat of cyberattacks without cooperation and proactive partnership as intelligence sharing between the public and private sector aid the mitigation and prevention of cyberattacks.[126] Examples of such collaboration is the Domestic Financial Fraud Kill Chain (DFFKC) between FIs and law enforcement. The IC3's Recovery Asset Team (RAT) operates within the DFFKC to facilitate the recovery of money lost by victims of Business Email Compromise (BEC)[127] scams through efficient communication with financial Institutions. In 2019, the IC3 RAT sent out notifications of 1,307 DFFKC's and was able to recover 79% of over $304 million lost.[128] Likewise, in 2018, the IC3 was able to recover 75% of over $250 million lost.[129]

A further good example of the interplay of criminal justice and regulatory responses in practice can be observed from the recent operation of the RAT in February 2019 in relation to a complaint raised by a BEC victim who in response to a spoofed email carried out a wire

[123] OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, 31.
[124] S M Kerner, 'Why JPMorgan Chase Data Breach May Have Financial Fallout' (*eWeek*, 5 October 2014) <https://www.eweek.com/security/why-jpmorgan-chase-data-breach-may-have-financial-fallout> accessed 31 July 2020.
[125] Majone, 'The rise of the regulatory state in Europe' 80.
[126] Ariana L Johnson, 'Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation' (2016) 20 North Carolina Banking Institute 277, 285.
[127] This is a type of scam whereby a hacker falsely deceives an organisation into wiring payments for a fraudulent invoice.
[128] IC3, '2019 Internet Crime Report' 10.
[129] IC3, '2018 Internet Crime Report' 11.

transfer of $138,000 to a fraudulent account. In addressing this complaint, the RAT communicated the complaint to the perpetrator's bank, who in turn notified law enforcement when the fraudster appeared at the bank to withdraw the transferred funds resulting in a prompt arrest of the fraudster.[130]

Equally, in February 2020, the US Department of Justice prosecuted 4 associates of the Chinese People's Liberation Army for a three-month targeted attack on Equifax's networks for theft of personal/sensitive data belonging to about 150 million Americans, as well trade secrets relating to its 'data records and database designs'.[131] While the outcome of the prosecution is uncertain, it is hope that this would serve two purposes. First, as a deterrent to cybercriminal conduct. Second, as a reminder to US legislators on the longstanding need for a detailed and uniform data breach notification standard. Indeed, it has been observed that security in the US is frustrated by a muddle of data protection laws and regulators each with limited obligations.[132]

In summary, though the US financial regulatory structure is arguably inherently problematic in nature, the sector has recorded a few regulatory successes in terms of enforcement of sanctions and prosecution of cybercriminals, especially due its collaboration with the Justice Department as it is subject to regulation under a broad array of legislation prescribing cybersecurity requirements. This is discussed in the next section.

5.7 National and International Cybersecurity Standards Applicable to US FIs

In addition to regulatory guidance and organisational policies, a number of federal and state legislation as well as national and international standards, set out requirements relating to cybersecurity in the US financial services sector.

[130] IC3, '2019 Internet Crime Report' 11.
[131] US DOJ, 'Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax' (10 Feb 2020) <www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking> accessed 23 July 2020.
[132] J. Kleinig and others, *Security and Privacy: Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States* (ANU E Press 2011) 57.

The National Institute of Science and Technology Cybersecurity Framework

The National Institute of Science and Technology (NIST) is a US Cybersecurity Framework (CSF) which sets out guidance for best cybersecurity practices which organisations and businesses may adopt. It identifies five relevant cybersecurity risk management functions i.e. identification, protection, detection, response and recovery. The NIST CSF aims to create a robust approach as each function is to be incorporated into an organisations processes and activities which may help organisations to develop best practice policies and has been followed by other countries including Japan, Israel and Italy as well as institutions in various sectors.[133]

The US NIST CSF and the FFIEC CAT are tools which banks may voluntarily use in the assessment of cyber-risk.[134] The CSF has 5 key functions, broken down into 22 components which are further broken down into almost a hundred cybersecurity control functions. Examples of NIST CSF components which should be included in the cyber risk regulatory and management framework of FIs include business environment, governance, risk assessment, risk management strategy, training and awareness, access control, data security, detection processes, security continuous monitory, response planning, communications, analysis, mitigation, improvements and recovery plans.

In its 2018 Framework for Improving Critical Cybersecurity Infrastructure, the NIST sets out four implementation tiers to provide context on the perceptions of cyber risks and management processes and how a dimensional move in the tiers would invariably help an institution in a cost-effective reduction of cyber risk. This is represented in the figure below:[135]

[133] Nicole Keller, 'Picking Up the Framework's Pace Internationally' (2019) <https://www.nist.gov/cyberframework/picking-frameworks-pace-internationally> created 13 June 2019 and accessed 12 October 2019.
[134] FFIEC CAT is based on the NIST and strictly for FIs.
[135] NIST, 'Framework for Improving Critical Infrastructure Cybersecurity Version 1.1' (16 April 2018) 9 <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> accessed 12 October 2019.

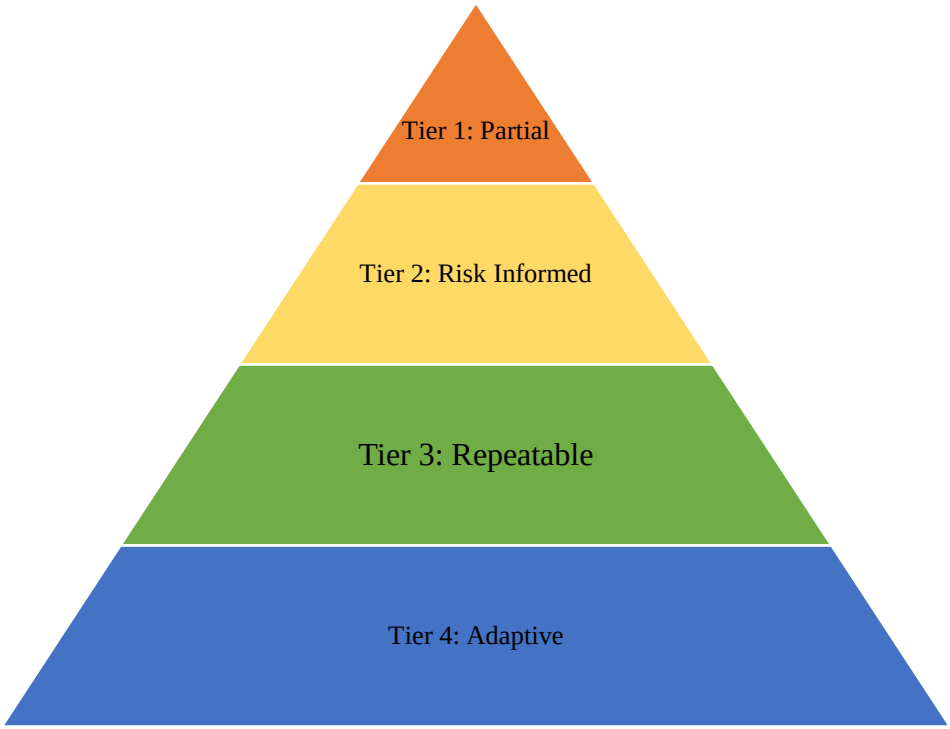

Figure 5-3 *NIST CSF Implementation Tiers*

Tier 1 institutions possess partial risk management procedures i.e. unorganised risk management procedures, erroneous risk management plans, and no external input towards risk management in the environment. Tier 2 institutions risk management procedures are risk-informed but possess risk management practices below standard, weak risk management procedures, and limited understanding and involvement towards their role in the risk environment. Tier 3 institutions carry out repeatable risk management practices. They possess systematic risk management procedures, robust risk management systems, and are routinely involved in risk management within the ecosystem. Tier 4 institutions carry out adaptive risk management practices. They employ continuously improved risk management procedures, flexible risk management systems, and regularly contribute and communicate within the risk environment.

Despite the comprehensiveness of the framework, the NIST CSF has been criticised for its broad prescriptions, voluntary nature and the ambiguity of the implementation tiers

such that they cannot be put to use.[136] In contrast, some studies suggest that assessing compliance of selected tiers to the NIST CSF help to identify gaps to be addressed in business areas for mitigating security threats.[137] Truly, we observe the specifications of Tiers 3 and 4, and identify adaptive practices and interactions, which Beck describes as "developmental variants which transform the modernization process itself into a learning process, in which the revisability of decisions makes possible the revocation of side effects discovered later."[138] With respect to strengthening resilience to third-party operational risk, FIs are advised to implement repeatable processes which in time form part of the organisational culture and arguably help to navigate the existing and conflicting standards in place.[139]

Committee on Payments and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO)

As a member of the CPMI-IOSCO, the US in 2016, adopted the "Guidance on cyber resilience for financial market infrastructures".[140] This Guidance focuses on the strengthening and promoting international uniformity in the sector's continuous endeavours to improve Financial Market Infrastructures' (FMI) capacity to mitigate cyberattacks, respond promptly and adequately to them, and accomplish quicker and more secure target recovery plans in successful attack.[141]

The Guidance sets out standards to be adopted for identifying, protecting, testing against, detecting, responding and recovering from cybersecurity risks. Some key provisions contained in the guidance require active engagement of board and senior management in the assessment of the FIs risk profile and implementation of its cybersecurity strategies[142], the

[136] Craig Jackson, Scott Russell and Bob Cowles, *Beyond the Beltway - The Problems with NIST's Approaches to Cybersecurity and Alternatives for NSF Science* (Center for Applied Cybersecurity Research 2017) 17.
[137] Ahmed Ibrahim and others, 'A security review of local government using NIST CSF: a case study' (2018) 74 The Journal of Supercomputing 5171, 5184.
[138] Beck and others, *Risk Society: Towards a New Modernity*, 178.
[139] John Haller and Charles Wallen, *Managing third party risk in financial services organizations: a resilience-based approach* (Carnegie Mellon University Software Engineering Institute September 2016) 8.
[140] International Monetary Fund Western Hemisphere Department, *United States: 2019 Article IV Consultation - Press Release; Staff Report; and Statement by the Executive Director for the United States* (INTERNATIONAL MONETARY FUND 2019) 78.
[141] Bank for International Settlements (BIS), 'Guidance on cyber resilience for financial market infrastructures' (29 June 2016) <https://www.bis.org/cpmi/publ/d146.pdf> accessed 15 August 2018 (BIS Cyber Resilience Guidelines for FMIs).
[142] ibid para 2.3.1.

assessment of insider threats to the security of systems and customer data[143], timely reporting of cyber incidents and conducting testing programmes.

In particular, the guidance prescribes a reflexive practice by which the response and notification plan to be implemented must be formed and informed through a consistent scenario-based exercise, evaluation and prior knowledge and then communicated to regulators, service providers, affected persons and other key partners.[144] Likewise, any tests conducted must involve various stakeholders and users of the systems, services, products or information of the institution such as incident and crisis response teams and service providers etc.[145] Thus, emphasising the need for participation and network in cybersecurity regulation. An example of such collaborative testing is the FS-ISAC CAPS exercise.

5.8 Criminal Justice Responses Applicable to US FIs Under Legislation

International Response to Cybercrime

Budapest Convention on Cybercrime

The US signed the convention in November 2001, ratified it in September 2006 and it came into force in January 2001. The Convention requires that its signatories adopt a number of measures including enforcement of 'effective, proportionate and dissuasive' sanctions,[146] real-time collection of computer data,[147] and cooperation among parties to the convention.[148]

A major setback of the Convention for the US is the failure of countries[149] which commonly target the US for hacking to sign the convention, thus leaving them out of any related substantive and procedural law requirements, including the extradition of computer criminals.[150] Truly, the lack of harmonisation of national laws tend to weaken enforcement efforts, since the cybercrime law in each country may vary differently.

[143] ibid para 4.4.1.
[144] BIS Cyber Resilience Guidelines for FMIs, para 6.4.3.
[145] ibid at 7.2.2(a).
[146] Council of Europe Convention on Cybercrime, Article 13.
[147] Council of Europe Convention on Cybercrime, Article 20.
[148] Council of Europe Convention on Cybercrime, Article 23.
[149] Countries include Russia, China, North Korea and Iran.
[150] J. Kosseff, *Cybersecurity Law* (Wiley 2019) 267.

Domestic Legislation/Regulation relating to Cybersecurity for FIs

Banks and their third-party service providers are regularly reviewed by the FRS, the OCC, and the FDIC on their cybersecurity programmes and compliance with relevant laws.[151] There is no universal legislation which makes a FIs failure to implement cybersecurity frameworks, a criminal offence. However, there are laws addressing cybersecurity standards and requirements for financial services institutions and corresponding sanctions in the event of a breach. These include the Financial Services Modernization Act of 1999 (GLBA),[152] Dodd-Frank Act 2010, Sarbanes-Oxley Act 2002 and the Red Flags Rule.[153] As will be seen across the legal frameworks, there is a high-level expectation on board of directors and senior management to take responsibility for overseeing their organisation's cybersecurity risks and controls.

The Table below sets forth the relevant laws which provide cybersecurity requirements for US FIs to follow.

Sarbanes-Oxley Act 2002	• Requires full disclosure/reporting of possible weaknesses in IT system controls. • Institutional integrity in the public sector.
GLBA 1999	• Minimum operation processing obligations for bodies including financial institutions. • Controls enhancing data privacy and protection in financial institutions. • Disclosure requirement for security breaches.
Fair and Accurate Credit Transactions Act 2003	• A written identify theft prevention program. • Periodic review of the program to reflect risks. • Oversight of outsourcing risks.
Cybersecurity Information Sharing Act 2015	• Sharing and exchange of cyber threat indicators and measures. • Liability protections and exceptions in relation to information shared by institutions.

[151] FRS Enhanced Cyber Risk Management Standards.
[152] 15 U.S.C. 6801 - 6809.
[153] FRS, 'Information Technology Guidance' <https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm> accessed 18 August 2019.

- Requires removal of personal information that is unrelated to threat shared.

Table 5-5 *US Laws Specifying Cybersecurity Best Practices*[154]

Sarbanes-Oxley Act 2002

The Sarbanes-Oxley (SOX) Act was introduced in 2002 to address cases relating to abuse of power by management in US organisations and inaccurate external audit reports by establishing a process for audit and compliance enforcement.

Under the SOX, the Public Companies Accounting Oversight Board (PCAOB) was created to monitor, review and investigate the accounting and financial reporting standards adopted by publicly held institutions and enforce sanctions in the event of a breach, subject to the SEC's jurisdiction.[155] The PCAOB, though possessing authority under statute, is a board exercising delegated regulatory powers and not a governmental agency which in effect, leaves room for regulators to overrule its decisions in certain cases. For instance, under Section 104 of the SOX Act, companies which do not agree with the PCAOB's decision may request a review from the SEC.

The Cybersecurity Systems and Risks Reporting Act is a bill currently before Congress to amend the SOX Act, two sections of which relate to data security, management and disclosure.[156] Section 302 of the SOX Act requires a company's CEO and chief financial officer to ensure that there are effective internal control systems in place for the protection against data compromise by unauthorised persons and to ensure the controls are reviewed regularly.[157] Section 404 of the Act further requires that the annual audit of the firm's internal security controls be conducted independently by an external firm with all data being submitted to auditors, including those relating to security breaches.[158] If effectively implemented, the Act will further enhance the compliance of institutions to set up robust

[154] Example adapted from D.L. Cannon, *CISA Certified Information Systems Auditor Study Guide* (Wiley 2009) 17.
[155] Sarbanes-Oxley Act 2002, Section 103.
[156] United States Congress, 'H.R.5069 - Cybersecurity Systems and Risks Reporting Act' <https://www.congress.gov/bill/114th-congress/house-bill/5069/text> accessed 11 October 2019.
[157] Initial provision contained in 15 U.S.C. 7241.
[158] Initial provision contained in 15 U.S.C. 7262.

cybersecurity controls to safeguard the availability, confidentiality and integrity of customer data.

Overall, the SOX seeks to enhance the transparency and accountability of public companies by enforcing the responsibility of management for quality financial disclosures with sanctions[159] for related violations.

Gramm-Leach-Bliley Act 1999

The *GLBA* was enacted with the aim of providing a progressive risk management framework by which 'financial institutions' upheld the protection of customer privacy i.e. how consumers' financial information were being stored, used or distributed. The Act provides requirements subject to the FTC's[160] jurisdiction for FIs to give notice to their customers about privacy requirements with respect to their private personal financial data (Financial Privacy Rule)[161]; and to set up, "implement and develop a written information security program" that safeguards customers' personal financial information from probable threats/risks which have been identified and test the appropriateness of safeguards in place (Safeguards[162]). The Act further provides an obligation to ensure the "security and confidentiality of customers' non-public personal data."[163]

The Act also sets out a requirement similar to the Rule 30 of SEC's Regulations S-P, for federal financial regulators to prescribe regulations for the safeguard of customer data.[164] In 2001, US financial regulators implemented this provision by issuing a set of "guidelines for establishing standards to protect customer information which was subsequently amended in 2005 to include requirements for notifying customers after a breach."[165] This is also known as the Safeguards Rule. Through this rule, regulators are able to carry out enforcement actions on FIs who fail to develop and incorporate standard

[159] Sanctions may include civil fines up to $100,000 and $2,000,000 for natural persons and other persons respectively. For conducts committed intentionally, knowingly or repeatedly, sanctions may include $750,000 for natural persons and $15,000,000 other persons.
[160] A US independent authority whose objective is to ensure consumer protection, healthy and strong competition in financial markets and the enforcement of consumer protection and antitrust laws.
[161] 16 C.F.R. 313.
[162] 16 C.F.R. 314.
[163] 15 U.S.C. 6801.
[164] Gramm-Leach-Bliley Act 1999, Section 501(b).
[165] FRS Interagency Guidance for response programs for unauthorised access.

cybersecurity frameworks. Under the GLBA, fines of up to $100000 for institutions and $10,000 for individual officers may be imposed for *each* breach. As such, accountability of senior management and board directors as well as security control processes for the management of risk in institutions are then developed.

The Act also grants each federal banking authority the power to enforce Section 6285 of the GLBA against all FIs under their corresponding jurisdictions. This section provides that:

> "[relevant agencies] shall prescribe such revisions to such regulations and guidelines as may be necessary to ensure that such FIs have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect activities. . ."[166]

This provision as seen earlier has been enforced to cover instances of data breaches, where FIs fail to put in place appropriate frameworks for safeguarding consumer data. That being said, the adequacy of data protection under the GLBA has been widely debated.[167] While this law does offer some protection, in the wake of the Equifax cybersecurity breach, considerations are ongoing in the US Senate for the creation of privacy and data protection obligations to address gaps in legislation.

Fair and Accurate Credit Transactions Act 2003

The Fair and Accurate Credit Transactions Act (FACTA) requires proper disposal of customer information.[168] The FACTA sets out a requirement for FIs to implement an identity theft "red flags" prevention program.

---

[166] 15 U.S.C. 6825.
[167] Peter Heyward, 'Citigroup to Congress: Never Mind! (Some reflections on the Gramm-Leach-Bliley Act prompted by Citigroup's exit from insurance underwriting)' (27 June 2005) 8 <https://www.venable.com/files/Publication/8d8da029-f4c3-4d37-9afa-2d9213dfc017/Presentation/PublicationAttachment/d6105a2e-bbd1-4c73-a265-8070f38d69d0/1335.pdf> accessed 21 July 2020.
[168] Federal Trade Commission, "FACTA Disposal Rule Goes into Effect June 1" (1 June 2005) <https://www.ftc.gov/news-events/press-releases/2005/06/facta-disposal-rule-goes-effect-june-1> accessed 21 July 2020.

The Red Flags Rule also known as Identity Theft Rule has three components: risk-based regulation, guidelines and a supplement. The Rule mandates regulated institutions to develop a *written* identity theft program for its all its customer accounts subject to its scope and any relevant factors. Red Flags may comprise of alerts or warnings from a consumer reporting agency, notifications from customers, businesses, law enforcement agencies or victims of identity theft, suspicious personal identification information, suspicious activity on a related account and use of suspicious documents. This program must be reviewed from time to time and contains provisions for the detection, mitigation and prevention of identity theft, including:

> ensuring the program (including the Red Flags determined to be relevant) is updated periodically [undergoes repeatable adjustments], to reflect changes in risks [on the basis of learning] to customers and to ensure the safety and soundness of the financial institution or creditor from identity theft.[169]

In addition, credit agencies or FIs are required under this programme to "train staff, adequately for the effective implementation of the programme and exercise appropriate and effective oversight of service provider arrangements".[170] There are no criminal penalties for non-compliance to the Rule, but a breach of the rule may result in a maximum civil penalty of $3,500 per violation under FACTA.[171] If enforced appropriately, the Red Flags Rule may help FIs in developing reflexive practices which address some issues of effective change management and outsourcing risks.

Bank Service Company Act 1962

While not directly specifying cybersecurity requirements, the provisions on contractual or related services in the Act imply that third-party providers are to be regulated in the same manner as their contractors, meaning they too should be subject to cybersecurity best practices required by financial institutions. Section 1867 (c)(1) and (2) states that:

[169] 16 C.F.R. 681.1(d)(2)(i) – (iv).
[170] 16 C.F.R. 681.1(e)(3) and (4).
[171] 16 C.F.R. 1.98 and 15 U.S.C. 1681(a)(2)(A).

> whenever a bank that is regularly examined by an appropriate Federal banking agency, or any subsidiary or affiliate of such a bank that is subject to examination by that agency, causes to be performed for itself, by contract or otherwise, any services authorized under this chapter, whether on or off its premises –
>
> such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the bank itself on its own premises, and the bank shall notify such agency of the existence of the service relationship within thirty days after the making of such service contract or the performance of the service, whichever occurs first.[172]

Hence, pursuant to these provisions, third-party financial service providers in the US are reasonably expected to be held to the same cybersecurity standards required by the banks.

Cybersecurity Information Sharing Act 2015

The Act designates the DHS as a sole information portal for the unified sharing of information. It contains several privacy provisions for the purpose of regulating how sensitive and personally identifiable information is being shared.

The introduction of the CISA is of great significance as it addresses the private sector's long-time unwillingness to share security threat information due to legal considerations such as compliance with relevant privacy legislation where information shared could be released *via* a Freedom of Information Act request, such that privacy might be relinquished when information is shared and may result in a civil liability or enforcement action.[173] Of relevance, the act provides liability protections for FIs engaged in cyber threat information sharing and exchange with other stakeholders or the government, as an incentive

[172] 12 U.S.C. 1867 (c)(1) and (2).
[173] Alston & Bird, Cyber Alert, 'The Cybersecurity Information Sharing Act Is Now Law' 1 (23 December 2015) <https://www.alston.com/-/media/files/insights/publications/2015/12/icyber-alerti-the-cybersecurity-information-sharin/files/view-alert-as-pdf/fileattachment/15443cybersecurityinformationsharingact.pdf> accessed 10 December 2020.

to enhance detection and prevent or mitigate any potential outcomes in the event of a cyberattack.[174]

Cybersecurity Legislation at State-level

Griggs and Gul examined the protection of the financial sector and customers from cyber threats and attacks by requirements set out under New York State Cybersecurity Regulations noting its prospects of becoming a nation-wide standard for cybersecurity risks management involving to financial data.[175]

Several states in the US have specific legislation and regulations which set out requirements for data protection, cybersecurity and disclosure by financial institutions. For instance, the New York's Department of financial services, implemented its Cybersecurity Regulation (*23 NYCRR 500*).

The Superintendent of the New York's Department of financial services is responsible for enforcing its cybersecurity regulatory framework. The regulation imposes cybersecurity requirements covering risk assessments,[176] limitation of access privileges to non-public information,[177] audit trail,[178] limitation to data retention of non-public information,[179] security policies for third party vendors,[180] incident response plans[181] and reporting material cyber breaches to the superintendent within 72 hours[182].

While the importance of data breach notification requirements cannot be underestimated in light of incident monitoring, response and recovery, individual requirements across different US states may produce inconsistency and a compliance challenge where there are conflicting requirements for FIs who operate within different states. Indeed, some scholars have argued that such approach leads to a regulatory patchwork where

[174] CISA at 106(a) - (b), 105(c), (1)(b).
[175] G Griggs and S Gul, 'Cybersecurity threats: What retirement plan sponsors and fiduciaries need to know—and do' (2017) 24 Journal of Pension Benefits: Issues in Administration 17, 19.
[176] 23 NYCRR 500, Section 500.09.
[177] 23 NYCRR 500, Section 500.07.
[178] 23 NYCRR 500, Section 500.06.
[179] 23 NYCRR 500, Section 500.13.
[180] 23 NYCRR 500, Section 500.11. See Anton N Didenko, 'Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond' (2020) 25 Uniform Law Review 125, 165.
[181] 23 NYCRR 500, Section 500.16.
[182] 23 NYCRR 500, Section 500.17.

institutions will have to consider each relevant statute especially in instances where there has been a widespread data breach across states requiring different responses.[183]

Personal Data Notification and Protection Act of 2017

In the US, various Personal Data Notification and Protection Acts (PDNPA) have been introduced in Congress for the purpose of establishing a single national standard by which institutions may inform relevant authorities and customers of a data breach. However, neither of the bill was passed into law including the Personal Data Protection and Breach Accountability Act of 2014 aimed at sanctioning breaches to customer data protection, timely notification relevant parties as well as privacy and security requirements.[184] A key impediment to a federal US law is argued to be the right of states as legislation from the former may hamper the latter, with federal law being less or more restrictive than state law and thus undermining or strengthening the protections of citizens respectively.[185] In light of our current discussion, a PDNPA is necessary to ensure that customers are protected from the impacts of data breaches and that criminal actions may be initiated against institutions.[186]

Currently in the US, there are conflicting data breach laws at state level in the absence of a federal law. States have followed considerably divergent approaches to data breach notification with respect to timing, notification of affected consumers and authorities.[187] For instance, some states set the requirement for the notification to a regulator depending on the number of customers affected and perceived impact of the risk. With regards to the customers, notification without unreasonable delay is set in most states, whereby deadlines range between 7 to 60 days' notice.[188] Such differences extend even to penalties where the maximum penalties could range between $500 to $1000.[189] In the UK, the situation is very different with the existing Data Protection law offering higher penalties,

[183] J.P. Hutchins and others, *U.S. Data Breach Notification Law: State by State* (American Bar Association, Section of Science & Technology Law 2007) U.S. Data Breach Notification Law: State, xi.
[184] P. Burkart and T. McCourt, *Why Hackers Win: Power and Disruption in the Network Society* (University of California Press 2019) 43.
[185] Chlotia Garrison and Clovia Hamilton, 'A comparative analysis of the EU GDPR to the US's breach notifications' (2019) 28 Information & Communications Technology Law 99, 106.
[186] Burkart and McCourt, *Why Hackers Win: Power and Disruption in the Network Society*, 44.
[187] US Senate, 'Equifax Report' 12.
[188]Garrison and Hamilton, 'A comparative analysis of the EU GDPR to the US's breach notifications' 109.
[189] ibid 111.

fines of up to €20 million, or 4% of *annual global turnover*,[190] notification to regulators "where feasible within 72 hours and without undue delay"[191] and notification to customers without undue delay.[192]

There are great risks associated with the piecemeal state data breach notification requirements stemming from the absence of a federal data protection law in the US. Compared to UK where there is better coherence in data protection and privacy regulation, reflecting regulatory influence and initial improvements in the regulation of security failings within its financial institutions, the US seeking to protect state rights has opened up its financial services sector to conflicting and arguably inadequate approaches to data breach regulation. As such, a starting point in addressing this issue may be the implementation of legislative proposals requiring the passage of a National Data Security and Privacy Protection Law setting a uniform framework and minimum standards for the gathering, preservation, usage, and transmission of personal and sensitive data such as account numbers, debit/credit card numbers, login credentials and secure access codes, allowing access to any such account.

5.9 Possible Challenges to Reflexivity in US FI Cybersecurity Regulation

As far as the US framework is concerned, we observe a similar pattern to that of the UK framework, where challenges to reflexivity in its cybersecurity regulation include factors such as duplicity in regulatory functions, voluntary cyber incident reporting structures, conflicting cybersecurity requirements in states and lack of a uniform standard for data privacy and protection, some of which have been discussed earlier. Therefore, in this section, we briefly address the issue of inadequacy of cyber reporting requirement under legislation which has great implications for reflexive governance in the sector.

Inadequacy of Cyber Reporting Requirement Under Legislation

As mentioned, cyber incident reporting guidelines are voluntary. Unlike the UK's DPA 2018 which generates implications for FIs in relation to data breach notifications, the US has no such uniform requirement. Given that, FIs have the discretion on whether to implement

[190] Compliant with the GDPR, Article 83.
[191] Data Protection Act 2018, Section 67.
[192] Data Protection Act 2018, Section 68.

guidelines or not, and making the wrong choice could increase cyber risks. In light of reporting delays observed with Equifax, it is therefore crucial to push for binding rules requiring timely notification of cyber incidents in FIs and their associated providers. This is particularly important as regulators in their proposal for a cyber incident notification requirement estimate the submission of nearly 150 notification incidents annually, based on its evaluation of existing SARs and supervisory data on cyber incidents against banking institutions.[193]

The Interagency Guidelines Establishing Information Security Standards codified at sections 6801 and 6805(b)(1) of the Gramm-Leach Bliley Act, provide primary requirements for an FI to "notify its primary Federal regulator as soon as possible when [it] becomes aware of an incident involving unauthorized access to or use of sensitive customer information".[194] The requirements for notification of cyber incidents relating to 'unauthorized access to or use of sensitive customer information' offers a limited range and may not be interpreted to cover cyber incidents which do not involve access to/use of customer data, despite having far reaching consequences. Further, the timing of the notification i.e. as soon as possible, appears too broad, causing the likelihood of different interpretations by different FIs. Hence, in adopting specific incident reporting requirements, regulators must give weight not only to the content and timing of the notification, but also relevant sanctions for the violation of such requirements.

Lobbying

An aspect of the US regime which is not without controversy is its lobbying system. While the details of the lobbying are not relevant to this discussion, some key characteristics and views are worth highlighting as there are similarities in its possible implications and the implications of corruption highlighted in the Nigerian chapter which arise as a result of misuse of powers by public officials.

Lobbying may be viewed as a legal instrument for shaping public policy making. The current federal legislation governing lobbying in the US is the Lobbying Disclosure Act

[193] Joint Proposed Computer-Security Incident Notification Rules, 2304.
[194] 12 C.F.R. 30, Appendix B, suppl. A.

1995 primarily concerned with disclosure through registration and disclosure guidelines, with a number of amendments to the legislation occasionally driven by political scandals involving lobbyists and legislators.[195] It has been a component of democratic systems for more than two centuries.[196] Lobbyists are perceived as far more informed in their fields of expertise than a legislator would which helps prevent avoidable errors on the part of legislators.[197] Lobbying is however, closely connected to corruption. For instance, where lobbyists run fundraisers for a re-election campaign or make donations with the aim of influencing the policy and political landscape, this can lead to bias in policy making if boundaries are not set. Indeed, Basu and Cordella note that there are no clear-cut boundaries between corrupt and non-corrupt lobbying in the US, particularly as cases in the US sometimes involve corrupt lobbying in which huge and direct donations are made to politicians pave way for the contributions of lobbyist in drafting industry-friendly legislation.[198] In the same way, the common practice of the "revolving door" in which a legislator or public official becomes a lobbyist immediately after leaving public service can undermine the integrity of the system and lead to inefficiency in policy making where the official promotes their private interests over the interests of the general public.[199] To address these shortcomings, it is therefore vital to implement legal solutions such as prohibiting fundraising events and introducing a statutory time limit between leaving public office and lobbying.[200] Moreover, there is legislation in about 50 US States which make it unlawful for lobbyists to make direct donations to any public official or legislator and/or for any public official to solicit for or accept any donations.[201]

It is believed that transparency/disclosure of lobbying is not an incentive to sufficiently fulfil public interest goals, and that issuing code of ethics may be required to tackle scandalous forms of undue influence, for example, the US, in addressing the recent

[195] Craig Holman and William Luneburg, 'Lobbying and transparency: A comparative analysis of regulatory reform' (2012) 1 Interest Groups & Advocacy 75, 80.
[196] OECD, 'Lobbying in the 21st Century: Transparency, Integrity and Access' (2021) 18.
[197] Caleb Lyle, 'Lobbying: An Overview and Outlook' (2020) Metamorphosis 1, 3.
[198] Kaushik Basu and Tito Cordella, *Institutions, Governance and the Control of Corruption* (Springer 2018) 118.
[199] Lyle, 'Lobbying: An Overview and Outlook' 8 - 9.
[200] ibid.
[201] National Conference of State Legislatures, 'Legislator Gift Restrictions' (13 September 2021) <https://www.ncsl.org/research/ethics/50-state-table-gift-laws.aspx#:~:text=No%20professional%20lobbyist%20shall%20knowingly,professional%20lobbyist%20shall%20not%20be> accessed 20 January 2022.

Abramoff lobbying scandal,[202] issued a number of ethics guidelines barring donations/gifts and funded travel from lobbyists to top public officials, legislators and their employees.[203] As we will see in the next chapter, corruption brings about almost similar implications as lobbying. Although, the implications for both systems are substantially different in that the focus of this thesis is on how regulations work in practice as opposed to how the systems arrive at these regulations. That is, while lobbying in the US typically impacts on the pre-implementation stage of the legislative process, corruption in Nigeria adversely affects both the pre and post implementation stages of the process i.e. the making and enforcement of the law. Moreover, in respect of the research at hand, there is no evidence to suggest a direct link between lobbying and the implementation of cybersecurity regulations in the US.

5.10 Conclusion

Mapping a reflexive approach for appropriately tackling cyber risks in the US financial services sector entails consideration of a number of factors. These factors such as comparability, consistency, intention, controlled flexibility and harmonisation in its security regulation may open up critical opportunities to mitigate evolving cyber risks and build repeatable systems.

The chapter shows a combination of both reactive and proactive regulatory approaches to cybersecurity, hence supporting the argument in Chapter 3 and 4, that one cannot exist without the other to achieve reflexivity in the sector. Through some collaboration, we notice the co-existence between the sector and government in the communication and exchange of information for the purpose of enforcement. The Citigroup Data Theft also highlights how criminal justice responses may intervene upon failure to self-regulate and affirms the argument of self-regulation in the shadow of the law.

Further, we observe a heavy reliance of regulators on a number of voluntary guidelines which FIs may discretionarily apply. In this regard, we observe some inadequacies in existing cybersecurity regulatory requirements, particularly in incident reporting, which are

[202] The Abramoff scandal involved lobbyists Jack Abramoff and Michael Scanlon who charged tribes seeking to develop casino gambling on their reservations about $85 million for their lobbying work.
[203] Holman and Luneburg, 'Lobbying and transparency: A comparative analysis of regulatory reform' 101 - 102.

not suited to the reflexivity objective seeing that reproducible knowledge and repeatable practices serves to inform risk management decisions. As such, regulators must without further delay implement the proposed cyber incident notification rules, taking into account necessary recommendations, to advance the sector's knowledge and approaches to cyber risks towards ensuring effective regulation of such risks in FIs.

Cyberattacks are risky, prevalent, and global threats, which will continue to evolve exponentially. The existing regulatory structure in the US emphasises regulation by a multitude of regulators each with interfering cyber risk management guidelines that set the pace for confusion rather than coordination. Indeed, a plethora of regulators both at state and federal level causes resource and constraint costs and may lead regulators to overlook activities necessary for the monitoring and supervision of cyber risks. Having various levels of regulators and standards for the same sector in the same jurisdiction has been argued to lead regulators to either "catching too little or too much".[204] As such, a convergent approach to financial sector cyber risk management in US is needed to counter existing limits to achieving greater similarity and effectiveness in cybersecurity regulatory frameworks.

[204] I.H.Y. Chiu, *Regulatory Convergence in EU Securities Regulation* (Wolters Kluwer 2008) 135.

Chapter 6. Case Study Nigeria

6.1 Introduction

Within the last two decades, the introduction of IT in the Nigerian financial sector has fundamentally restructured financial services operations from manual to automated systems.[1] While this has led to an improvement in the efficiency, quality and growth of banking services, it has resulted in more sophisticated and technical risks.

In a report by the Carnegie Endowment for International Peace, cybercriminals in July 2016 carried out a theft of $100 million from a bank in Nigeria to banks in Asia, through the compromise of SWIFT transactions. The funds were eventually retrieved and the crime was later suggested by United Nations (UN) Security Council experts as being perpetrated by actors associated with the North Korean government. Similarly, in March 2019, cybercriminals attempted a theft of $12.2 million from a financial institution in Nigeria, which was also suggested as being perpetrated by actors associated with the North Korean government.[2] This comes as a surprise as there is almost no evidence in publications or reports by regulators confirming these attacks, despite their magnitude. It further raises questions on the practicability and enforceability of cybersecurity regulations in the Nigerian financial services sector.

In the previous chapters, we have considered how financial institutions in the UK and US co-exist and effectively self-regulate against the backdrop of the state and what the challenges were to an effective reflexive governance. This chapter will set the scene for the lessons to be learnt, evaluating the similarities as well as the differences of a developing jurisdiction against developed ones, addressing questions about the accountability of financial institutions for cybersecurity failings and the balance between self-regulation and criminal justice systems.

One may therefore learn lessons from the way in which the UK and US rhetoric have influenced the model of cybersecurity law and policy texts in Nigeria. In particular,

[1] Alhaji Abubakar Aliyu and RB Tasmin, *Information and Communication Technology in Nigerian Banks: Analysis of Services and Consumer Reactions* (2012) 152.
[2] CEIP, Timeline of Cyber Incidents Involving FIs (2020).

many of the shortcomings highlighted in the previous chapters though specific to each country, appear to also occur in Nigeria. This is largely due to the lack of implementation of effective cybersecurity practices, the roots of which have been deeply planted in governance failures. To this end, we first discuss the nature and effects of cyber risks on the Nigerian financial sector using the findings from the case studies of Guaranty Trust Bank Plc and First Bank Plc to identify the risks which they have experienced over time and the risk management framework adopted to address such risks. Although, banks in the other two jurisdictions were discussed in detail in the previous chapters, this chapter does not provide much detail due to the absence of adequate evidence in the current jurisdiction. Despite these limitations, it is believed that this chapter advances arguments sufficient enough to solve the hypothesis posed in this thesis.

In the final sections, we discuss the possible challenges to reflexive regulation in the Nigerian financial sector and defend the view that its major problem lies in its dubious replication of the UK and US models, accompanied by its multiplicitous institutional structures, and further aggravated by poor governance practices, legislative inadequacies and lax cyber incident reporting attitudes by FIs. These issues will be explored in much detail across section 6.7 and then resolved in section 6.8, through suggestions and proposals for reform.

6.2 Background and Institutional Framework of the Nigerian Financial System

Prior to 1960, Nigerian banks operated under the 'free-banking' and 'pre-regulation' era.[3] During this period, the banking operations were ineffective over failings of the West African Currency Board and the poor operational, technical and managerial standards of the indigenous banks.[4] In response, Nigeria passed its first banking legislation, The Banking Ordinance in 1952.[5] Subsequently, the Central Bank of Nigeria (CBN) was established in

[3] That is, the era where banks were left to carry out their operations without being subject to any restrictions under regulation. Muhammad Auwalu Haruna, 'Analysis of value creation of electronic banking in Nigeria' (2012) 46 International Journal of Advanced Research in IT and Engineering, 1 (2), 29, 31.
[4] Central Bank of Nigeria (CBN), 'Understanding Monetary Policy Series No 7 - Banking Sector Reforms in Nigeria' (July 2011) 7 <https://www.cbn.gov.ng/Out/2015/MPD/UNDERSTANDING%20MONETARY%20POLICY%20SERIES%207.pdf> accessed 31 March 2019.
[5] Thorsten Beck, Robert Cull and Afeikhena Jerome, *Bank privatization and performance: Empirical evidence from Nigeria* (The World Bank 2005) 6.

1959 to conduct regulation and control, towards maintaining the integrity and financial stability of the banking system. However, it was not until 2010 that reforms which focused on corporate governance, consumer protection and disclosure were considered.[6]

Between 1989 and 1998, Nigeria experienced consecutive rounds of financial crises, initially involving eight banks and subsequently resulting in the liquidation of thirty-one banks and leaving a further eighty-nine with fluctuating levels of financial soundness.[7] The financial crises, to a great extent, were attributed to bad corporate governance deeply rooted in frauds, money laundering, undercapitalisation, round-tripping and un-securitised insider loans.[8] This chain of failures led to a series of reforms in 2004, proposed by the then Governor of the CBN, Professor Charles Soludo. According to him, the problem of weak corporate governance in FIs was a product of non-compliance with regulatory standards, underreporting, gross insider abuse and non-publication and late publication of annual reports etc.[9] These issues, also influencing the growth of cybercrimes in Nigerian FIs, appear to play a recurrent role in their regulatory failures as will be seen later in this chapter.

The early approach to regulation in the Nigerian financial services sector was the command-and-control approach, reflective of the first two conceptualisations of regulation by Baldwin et al, as regulation exercised by state institutions using legal measures. By virtue of the 1952 Ordinance, the government was responsible for the management, examination and control of FIs[10], many of which were, state-owned and over-regulated by the CBN and Nigerian Deposit Insurance Corporation (NDIC) and in effect, made it impossible for FIs to initiate effective anti-inflationary measures.[11] FIs were also required to adhere to many laws and rules with threat of sanctions which were hardly imposed or ineffective. According to the former CBN President, Lamido Sanusi, enforcement was a major challenge to the CBN's

[6] Oluseun Paseda, 'Banking regulation in Nigeria: A review article' (2012) 25 International Organization of Scientific Research Journal of Humanities and Social Sciences 38, 53.
[7] Heiko Hesse, *Financial intermediation in the pre-consolidated banking sector in Nigeria* (The World Bank 2007) 7.
[8] A. Salawu and T.O.S. Owolabi, *Exploring Journalism Practice and Perception in Developing Countries* (IGI Global 2017) 26.
[9] Ngozi Okonjo-Iweala, *Reforming the unreformable: Lessons from Nigeria* (Mit Press 2014) 72.
[10] Godwin Chigozie Okpara, 'Bank reforms and the performance of the Nigerian banking sector: An empirical analysis' (2011) 2 International Journal of Current Research 142, 143.
[11] Chibuike Ugochukwu Uche, 'Banking regulation in an era of structural adjustment: The case of Nigeria' (2000) Journal of Financial Regulation and compliance 165.

examination processes as monetary penalties levied for non-compliance created a custom of lenience, were incapable of influencing conduct, and ultimately undermined the regulatory process.[12] This is confirmed by Akinyomi who notes that increase in fraud rates in Nigerian banks is enabled by factors such as a lack of penalties/sanctions imposed for non-compliance with specified policies.[13] This echoes the issues of systems monitoring, and enforcement highlighted by Black as the failures of such an approach.

The outcome of the 2008 financial crisis led to an increased attention of Nigerian financial regulators to self-regulation in the regulation of FIs and five years after, the Nigerian Banking Industry Code of Conduct[14] was crafted from the proposals made by the CBN.[15] The CBNs current approach of issuing guidance to banks on specific standards and objectives, indicate a shift from command-and-control to self-regulation. Particularly, its recent issuance of guidelines and standards on cybersecurity discussed in Section 6.5 reflect the self-regulatory style of influencing behaviours through procedures and strategies without direct government intervention.

Achua argues that a credible integration of corporate governance in the services of Nigerian FIs will be needed to ensure the success of self-regulation[16] and corporate governance is considered a fundamental component of cybersecurity.[17] However, studies on the effect of corporate governance on the conduct of FIs in Nigeria have shown that though banks were obliged to comply with the Codes of Governance, penalties for violations were not implemented[18], with a lack of effective enforcement exposing conflicts between objectives and practices.[19] Moreover, the lack or passive involvement of risk experts to inform

[12] LS Sanusi, 'The Nigerian Banking Industry: what went wrong and the way forward' (2010) 3 Delivered at Annual Convocation Ceremony of Bayero University, Kano held on 2010, para 2.7.
[13] Oladele John Akinyomi, 'Examination of fraud in the Nigerian banking sector and its prevention' (2012) 3 Asian Journal of Management Research 182, 188.
[14] The Chartered Institute of Bankers of Nigeria, 'Code of Conduct in The Nigerian Banking Industry 2013 (Professional Code of Ethics and Business Conduct)' <https://www.cibng.org/files/resourceDownloads/codeOfConduct.pdf> accessed 1 April 2021.
[15] Henry Chilewubeze Uzokwe, 'Consumer protection in the banking sector: the need for reform to protect bank consumers in Nigeria', Brunel University London (2017) 109.
[16] Joseph K Achua, 'Corporate social responsibility in Nigerian banking system' (2008) 3 Society and Business Review 57, 67.
[17]Rossouw De Bruin and SH Von Solms, *Cybersecurity Governance: How can we measure it?* (IEEE 2016) 4.
[18] Fatimoh Mohammed, 'Impact of Corporate governance on Banking Sector performance in Nigeria' (2011) 2 International Journal of Economic Development Research and Investment 52, 57.
[19] Alex Ehimare Omankhanlen and JN Taiwo, 'The role of corporate governance in the growth of Nigerian banks' (2013) 1 Journal of Business law and Ethics 44, 56.

vital decisions[20], deep-rooted corruption, impunity from prosecutions and convictions and poor regulatory mechanisms resulting from a system of patronage[21] have made it difficult to ensure good corporate governance and risk management practices in Nigerian banks. Under these circumstances, it is imperative to emphasise that self-regulation is not a cure for government regulation and does not imply an abolishment of the use of laws and sanctions, but mainly a complement to it. Therefore, if issues of accountability, transparency and governance are not addressed, there can be no development of self-regulation.

Model of Regulation in the Nigerian Financial Sector

Like the UK, Nigeria adopts the twin-peaks approach i.e., a regulatory arrangement which involves regulation by objective[22] and requires a separation of regulatory roles between regulators, such that each objective is the responsibility of a separate regulator.[23] There are three primary regulators, several supervisory, law enforcement and federal government authorities involved in the regulation and supervision of FIs in Nigeria. The regulatory agencies in the financial sector include the CBN, the Securities and Exchange Commission, the Nigerian Deposit Insurance Corporation (NDIC), the National Pension Commission, the National Insurance Commission, the Economic and Financial Crimes Commission (EFCC) and the Nigerian Financial Intelligence Unit (NFIU).

Of relevance to this research is the CBN and the NDIC mainly responsible for the supervision of banks, and supported by the EFCC and NFIU, responsible for enforcing the law.

[20] Kenneth I Ajibo, 'Risk-based regulation: The future of Nigerian banking industry' (2015) 57 International Journal of Law and Management 201, 208 - 209.
[21]Ayodele Adelaja Adekoya, 'Corporate Governance Reforms in Nigeria: Challenges and Suggested Solutions' (2011) 6 Journal of Business Systems, Governance and Ethics 38, 43.
[22] "an objective-oriented approach", see Ferran, 'The break-up of the financial services authority' 464.
[23] Godwin, Howse and Ramsay, 'A Jurisdictional Comparison of the Twin Peaks Model of Financial Regulation' 105.

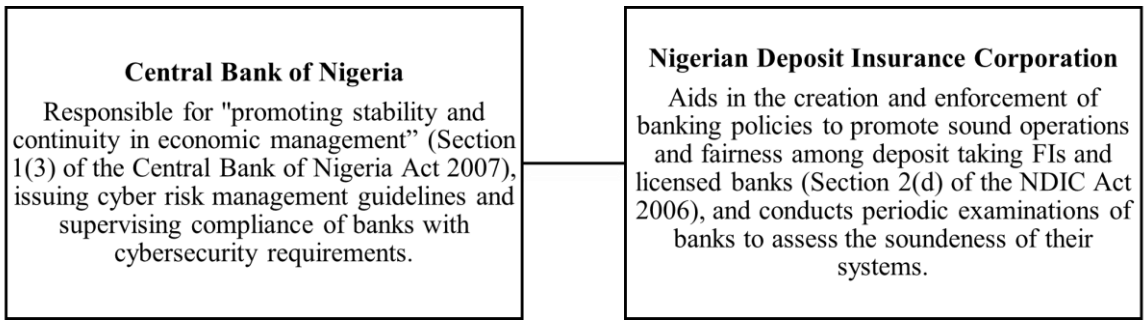

Figure 6-1 *Nigerian Financial Regulatory Approach to Cyber Risk Regulation*

The Central Bank of Nigeria

Formed in 1959 to ensure that commercial banking was carried out in a sound and systematic manner, the CBN is directly responsible for regulating and supervising FIs and specialised banks in the Nigeria as well as promoting the effectiveness of monetary policies. As a pre-independence institution, the CBNs ethos was shaped by the need to perform "developmental functions", and in particular enhance the "development of sound financial structures".[24] However, the invasion of its authority by the military government shortly after independence from 1966 to 1990[25] considerably affected its operations. Following the interference, the CBNs institutional performance was found to have fallen with its foundations deeply rooted in corruption engineered by institutions of the state.[26] This lax culture of the CBN may be argued to have given post-independence political leaders the powers to exercise control on its activities for the purpose of extending their wealth and hoarding investments. Indeed, the CBNs ability to fulfil its legal mandates have been found to be threatened by its lack of independence.[27]

The mandate of the CBN finds its origin in the Act of Parliament 1958, as amended several times, up until 2007. The 2007 Act was introduced to confront many issues, particularly those relating the CBNs independence and its impact upon their monitoring and supervision objectives. In addition to the functions identified in ***Figure 6-1***, other cyber-related objectives of the CBN include: to promote the soundness of the Nigerian financial

[24] Toyin Falola and Akanmu Gafari Adebayo, *Culture, Politics and Money Among the Yoruba* (Transaction Publishers) 295.
[25] C.S.K. Tardzer, *My Odyssey, My Country* (Xlibris US 2012) 225.
[26] F.O. Onamson, *Law and Creditor Protection in Nigeria* (Malthouse Press 2017) 74.
[27] M. Saxegaard and International Monetary Fund. African Department, *Excess Liquidity and the Effectiveness of Monetary Policy: Evidence from Sub-Saharan Africa* (INTERNATIONAL MONETARY FUND 2006) 18.

system; and, to serve 'as a banker and offer both economic and financial advice to the government'.[28]

As part of achieving these objectives, the CBN in 2012, moved to reduce the amount of physical cash circulation in the economy and promoted the use of e-banking systems. In view of this, a cashless policy was launched, and charges were specified on daily cash withdrawals below certain amounts for individuals and corporations to discourage transactions with physical cash, thus increasing dependence of the country on e-banking platforms. Given that, it became imperative for the country to put in place laws and guidelines to address existing and potential cybersecurity issues which may hamper or exploit the use of such platforms.

Since January 2012, only 2 of the 342 Financial Stability Supervision Circulars issued by the CBN addresses issues relating to cybersecurity in FIs. In contrast to the UK and US where cybersecurity risk supervision functions as a collective responsibility amongst its regulators, in Nigeria, this function is situated within the Banking Supervision Department of the CBN, which is responsible for receiving and managing cyber security risk reports from FIs.[29] Likewise, when compared against the UK and US, the cybersecurity guidelines issued in Nigeria reveal a lack of structural detail. As the Banking Supervision Department, responsible for enforcing these guidelines forms part of the CBN, issues of transparency and accountability arise seeing that there is no division of this responsibility across regulators. Indeed, the institutional structure of the Banking Supervision Department has been long known to affect its effective supervision and enforcement of regulations.[30] Hence, while the cybersecurity risk management guidelines introduce measures which if implemented correctly may inform reflexive practices, their effectiveness remains questionable if they are not supported by appropriate institutional structures.

[28] CBN Act 2007, Section 2(d) and (e).
[29] CBN, 'Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs)' (October 2018) para 5.6 <https://www.cbn.gov.ng/Out/2018/BSD/RISK%20BASED%20CYBERSECURITY%20FRAMEWORK%20FINAL.pdf> accessed 14 March 2019.
[30] "The Supervision Department within the CBN was not structured to supervise effectively and to enforce regulation". See Sanusi, 'The Nigerian Banking Industry: what went wrong and the way forward' para 2.7.

Nigerian Deposit Insurance Corporation

The NDIC is one of the regulatory agencies and the deposit insurer for FIs. While the NDIC has no specific mandate for cybersecurity supervision, it exercises its directive by conducting on-site and off-site examination of the operations of all licensed deposit taking FIs to assess risks to the soundness of the financial system and may issue guidance for prompt corrective action, where unsound practices are identified. Meanwhile, in its 2019 Annual Report, the NDIC acknowledges the significance of successful risk management in the sector and enhanced cybersecurity frameworks.[31]

By virtue of the NDIC Act 2006, banks are to provide detailed monthly reports on frauds to the NDIC.[32] Through this mandate, the NDIC oversees and enforces the obligation of FIs to take necessary precautions to protect their systems and customers against cybercrime in various ways such as, a 24-hour toll-free telephone line to allow report of any unlawful financial activity including cybercrime for investigation and the establishing of a Complaints department to resolve concerns of bank customers.[33]

Economic and Financial Crimes Commission

The EFCC is a Nigerian law enforcement agency which carries out the examination and investigation of all economic and financial crimes and the enforcement of all economic and financial crime laws[34].

The EFCC Act 2004 confers upon the EFCC wide powers to carry out investigations and launch prosecutions across a broad range of crimes. However, the broad enforcement and coordination powers granted to the EFCC in effect, creates friction in the institutional framework as these powers relate not only to economic and financial crime laws but also some cybercrime provisions, which by virtue of the Cybercrimes Act 2015, had been

[31] Nigerian Deposit Insurance Corporation (NDIC), '2019 Annual Report for the Year Ending December 31, 2019' para 13.2 <https://c5e9r5w9.rocketcdn.me/wp-content/uploads/2020/12/2019%20Annual%20Report%20Press.pdf> accessed 10 December 2020.
[32] NDIC Act 2006, Section 35.
[33] NDIC, 'The Impact of Cybercrime on The Nigerian Economy and Banking System' (March 2020) para 6.3 <https://ndic.gov.ng/wp-content/uploads/2020/03/NDIC-Quarterly-Q1-and-Q2-2019-Article-The-Impact-of-Cybercrime-on-The-Nigerian-Economy-and-Banking-System-.pdf> accessed 20 September 2020.
[34] Coordination and enforcement powers conferred by virtue of EFCC Act 2004, Section 6 (b) - (c).

placed under the mandate of the Nigerian Communications Commission. According to the EFCC Act, financial crimes consists of all traditional forms of financial crimes including money laundering, advance fee fraud, computer credit card fraud, illegal charge transfers and contract scams.[35] Prior to the creation of the new law, existing mandates relating to cybercrimes should have been reviewed to avoid a legal uncertainty.

The Act mandates the Commission to be responsible for the gathering, evaluation and communication of reports on suspected fraudulent financial transactions possibly relating to money laundering, fraud as well as cyber-enabled crimes to relevant federal agencies.[36]

In order to improve cooperation and confidence with foreign intelligence agencies; amend certain functions of the EFCC; develop organisational capacity; implement functional resolution of cases; and an establishment of an EFCC court, an Amendment Bill was proposed to the 2004 Act. Schedule 2(1) of the Amendment Bill 2016 provides for the establishment of an EFCC Court to preside over all cases relating to economic and financial crimes and other provisions of the Act[37] which would include proceedings on some financial cybercrimes which the 2004 Act makes provisions for. The importance of a financial crimes court proposed in the amended EFCC Act is yet to be conceived as the Nigerian judiciary has been found to have long-standing challenges resulting from executive interference. Judges in Nigeria are understood to receive bribes to fulfil requests from public officials to prolong or sometimes expedite cases and that legislators as well collect bribes and favours from the executive branch in exchange for passing a bill that is beneficial to them.[38] Obuah confirms that the amendment of regulations are oftentimes done with the aim of according benefits to either government or non-government actors in order to provide unlawful private advantages to public officials.[39] This suggests a problem of regulatory capture where the private interests of a few elite or wealthy class belonging to the same political groups are fulfilled over those of the public.

[35] EFCC Act 2004, Section 6(b).
[36] EFCC Act 2004, Section 6(l).
[37] EFCC Act (Amendment) Bill 2016, C 532, para 1.
[38] Emmanuel Obuah, 'Combating corruption in a "failed" state: the Nigerian Economic and Financial Crimes Commission (EFCC)' (2010) 12 Journal of Sustainable Development in Africa 27, 39.
[39] ibid 34.

The Commission encounters various institutional and regulatory challenges in the discharge of its functions. First, there is the presence of political interference to prolong its investigative processes and adjust its institutional structure.[40] An example of the latter was seen in the case of its pioneer Chairman who was removed from office under the pretext of being sent on a year's training programme to become an Assistant Commissioner of Police.[41] The EFCC has also been argued to lack independence due to its institutional structure under the 2004 Act, requiring an appointment of the Chairman and Secretary by the President.[42] The Act further vests upon the President, the power to terminate the appointment of the Chairman where he is satisfied that it is "in the interest of the organisation and the public that the individual vacates the office".[43] In addition, the EFCC has also been noted to lack funding and sufficiently trained personnel, such that the dominance of the police force within the institution were criticised as undermining its objectives due to their inherently corrupt reputation.[44]

Nigerian Financial Intelligence Unit

By virtue of the EFCC Act 2004, the NFIU was established to ensure the coordination of all institutions working towards combatting money laundering, terrorist financing and predicate offences to law enforcement and anti-corruption agencies in Nigeria.[45] In the UK and US, similar agencies have also been established namely the National Crime Agency (NCA) and the Financial Crimes Enforcement Network (FinCen), respectively.

In a recent submission made by the NFIU to the United Nations Office on Drugs and Crime, it claims that it coordinates with law enforcement bodies like the EFCC and Nigerian Police in the delivery of actionable intelligence to commence investigations and

[40] Emilia Onyema and others, 'The Economic and Financial Crimes Commission and the politics of (in) effective implementation of Nigeria's anti-corruption policy' (2018) 29 <https://ace.soas.ac.uk/wp-content/uploads/2018/11/ACE-WorkingPaper007-EFCC-Nigeria.pdf> accessed 4 May 2019.
[41] C.N. QC and others, *Corruption and Misuse of Public Office* (OUP Oxford 2011) 396.
[42] K. Olaniyan, *Corruption and Human Rights Law in Africa* (Bloomsbury Publishing 2014) 147.
[43] EFCC Act 2004, Section 3(2).
[44] Ibrahim Umar, Rose Shamsiah Samsudin and Mudzamir bn Mohamed, 'Ascertaining the effectiveness of Economic and Financial Crimes Commission (EFCC) in tackling corruptions in Nigeria' (2018) 25 Journal of Financial Crime 658, 665.
[45] EFCC Act 2004, Section 1(c).

facilitate existing investigations of unlawful activities including, cybercrimes.[46] In spite of these claims, the NFIUs mandate may be said to be inexplicit as its impact is unnoticeable in the financial sector, due to the overlap in its functions and those of the EFCC. Awhefeada et al confirms this, noting that its reporting function is shared with other reporting institutions[47], and that the NFIUs arrangement within the EFCC threatens its independence.[48] This fully reiterates the findings from Olayemi that law enforcement agencies in Nigeria encounter challenges relating to the duplication of roles in cybercrime activities.[49] Therefore, the NFIU needs to be empowered to ensure that it is fully abreast on financial intelligence policies, procedures and responses to cybercrimes. Without well-defined systems of operation, the agencies are unlikely to achieve utmost efficiency and cost-effectiveness.

6.3 Emerging Risks in the Nigerian Financial Sector

Prevalent Cybercrimes in Nigeria

According to the report *2017 Cybersecurity Report by Serianu,* Nigeria lost an estimated $649m to cybercrime in 2014 and with the shift to a 'Cashless Society', the country is expected to lose even more.[50] The *Report* lists out trends and groups them according to their impact namely: insider threats amounting to about $194m; hacking attacks valued at $130m; social engineering and identity theft estimated at $97m; email spam and phishing frauds costing about $78m; data exfiltration put at $65m; online fraud scam valued at $52m, and ransomware at about $33m. The President of the Nigerian Computer Society echoes the prevalence of DDoS and social engineering, as key threats to the financial sector in the year 2019 and notes insider threats, unpatched systems, and malware as some of the sector's

[46] United Nations Office on Drugs and Crime (UNODC), 'Comment on Good Practices, New Information on National Efforts and Recommendation with regards to the Meeting of the Open-Ended Intergovernmental Expert Group on Cybercrime (Submission from the Nigerian Financial Intelligence Unit (NFIU))' (March 2019) 3 <https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Comments/Nigeria_2.pdf> accessed 18 September 2020 (UNODC, NFIU Comment on Good Practices).
[47] The CBN, SEC, National Insurance Commission, and the Special Control Unit against Money Laundering.
[48] Ufuoma V Awhefeada and Ohwomeregwa Ogechi Bernice, 'Appraising the Laws Governing the Control of Cybercrime in Nigeria' (2020) 8 Journal of Law and Criminal Justice 30, 43.
[49] Odumesi John Olayemi, 'A socio-technological analysis of cybercrime and cyber security in Nigeria' (2014) 6 International Journal of Sociology and Anthropology 116, 121.
[50] Serianu, Nigeria Cybersecurity Report 2017: Demystifying the Africa Cybersecurity Poverty Line' 11 (2017) <https://www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf> accessed 9 November 2018.

primary risks.[51] One such example is the Lazarus group malware found to have attacked FIs in Nigeria and 12 other countries and behind the $851 million heist initiated against the Central Bank of Bangladesh in 2016.[52]

Insider threat is another issue affecting cybersecurity risk management in Nigerian banks due the ease of access to financial information by staff. The EFCC launched its first investigation on cyber-related insider abuse in 2014 involving a bank staff who connived with fraudsters to install a key logging device into the banks computer system to steal passwords and network configuration settings to access operations of the bank.[53] There was however, no record on prosecution and conviction in its published reports. Indeed, data published on crimes reported, investigated, prosecuted and convicted by the EFCC, suggests that only a small fraction of convictions are achieved in its investigation and prosecution of cybercrimes. The discretionary decision of the EFCC to investigate or to reject a petition has come under public criticism for its failure to provide a criteria upon which it bases its decisions.[54] This undoubtedly raises questions as to the genuinity of its discretionary decisions.

Through 2018, the EFCC charged about seven cases on insider abuse by bank staff to court and secured a few convictions, some of which involved cybercrimes.[55] A recent case on bank staff insider abuse brought before the court in 2019 involved a conspiracy in obtaining by false pretence the sum of £100,000 from a customer *via* transfer to a foreign bank account, under the guise of offering bureaux de change services.[56] The accused were granted bail in the sum of N500, 000[57] each with two sureties. Meanwhile, in a recent case involving an

[51] Adeyemi Adepetun, 'Nigerian banks spent N200b preventing cyberattacks in 2019' (*TheGuardian*, 9 January 2020) <https://guardian.ng/business-services/nigerian-banks-spent-n200b-preventing-cyber-attacks-in-2019/> accessed 13 January 2021.
[52] Kaspersky, 'Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies' (3 April 2017) <https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies> accessed 10 November 2018.
[53] EFCC, 'EFCC Arrests Three Suspected Fraudsters for Attempted Hacking' (31 August 2014) <https://efccnigeria.org/efcc/news/987-efcc-arrests-three-suspected-fraudsters-for-attempted-hacking> accessed 30 April 2019.
[54] Onyema and others, 'The Economic and Financial Crimes Commission and the politics of (in) effective implementation of Nigeria's anti-corruption policy' 27.
[55] EFCC, 'Court Jails Ex-Banker 12 years For N450m Fraud' (14 March 2018) <https://efccnigeria.org/efcc/news/3131-court-jails-ex-banker-12-years-for-n450m-fraud> accessed 29 March 2019.
[56] EFCC, 'EFCC Arraigns Two Access Bank Staff for £100,000 Fraud' (25 January 2019) <https://efccnigeria.org/efcc/news/3677-efcc-arraigns-two-access-bank-staff-for-100-000-fraud> accessed 30 April 2019.
[57] about £833 at the rate of £1 to N600.

individual, charged to court for hacking into a victim's email and fraudulently diverting the sum of N2 million[58], the court found it equitable to impose a cumulative fine of N320,000[59] and a restituted sum of N2 million to the victim or a jail term of 29 years, if fine conditions cannot be fulfilled.[60] A relative comparison on approaches adopted by judges in both cases indicate inconsistency in sentencing practices and raises questions as to the validity of the judicial process.

In the most recent report published by the Nigerian electronic Fraud Forum (NeFF), the financial sector in Nigeria recorded a high percentage of phishing attacks (55.56%), when compared with malware attacks (18.52%), ransomware attacks (14.81%) and DDoS attacks (7.41%).[61] While the 2016 report by the NeFF does not indicate the causes of phishing attacks specifically, it does mention the susceptibility of victims to giving away personal information, low customer awareness and new evolving channels which the cybercriminals take advantage of.[62] In particular, the report highlights various regulatory challenges including low stakeholder collaboration and cost of compliance.[63] Indeed, in a recent study of banks in Nigeria, Fadayo observed that factors impacting the rise of e-banking fraud in Nigerian banks include weak cooperation of banks with law enforcement, inadequate controls for new services, lack of staff awareness etc.[64]

Scale and Impact of Cyber Risks

About a decade ago, cybercrime was considered to be Nigeria's third largest 'industry'.[65] These findings were well supported by data from Sesan et al, estimating consumer financial losses to cybercrime at about N2,146,666,345,014.75 in 2010.[66] A similar report by the NDIC

[58] about £4,050.
[59] about £533.
[60] EFCC, 'Man Bags 29 Years for N2m Cyber Fraud' (6 May 2019) <https://efccnigeria.org/efcc/news/4184-man-bags-29-years-for-n2m-cyber-fraud-2> accessed 6 May 2019.
[61] Nigeria Electronic Fraud Forum (NeFF), 'A Changing Payments Ecosystem: The Security Challenge – Annual Report 2016' 33 <https://www.cbn.gov.ng/Out/2017/CCD/A%20CHANGING%20PAYMENTS%20ECOSYSTEM%20NeFF%202016%20Annual%20Report.pdf> accessed 9 November 2018.
[62] ibid 45.
[63] NeFF, 'A Changing Payments Ecosystem: The Security Challenge - Annual Report 2016' 74.
[64] Matthew Fadayo, 'An examination of e-banking fraud prevention and detection in Nigerian banks', De Montfort University 2018) 232.
[65] N. Kshetri, *Cybercrime and Cybersecurity in the Global South* (Palgrave Macmillan UK 2013) 77.
[66] about £3,577,777,241.69. See Gbenga Sesan, B Soremi and O Bankole, 'Economic cost of cybercrime in Nigeria' (2013) Cyber Stewards Network Project, Munk School of global affairs, University of Toronto 5.

reveal an increase in the total fraud losses across internet banking platforms, reported between the years 2017 to 2018, followed by a sharp decrease in the year 2019, as shown in the figure below.

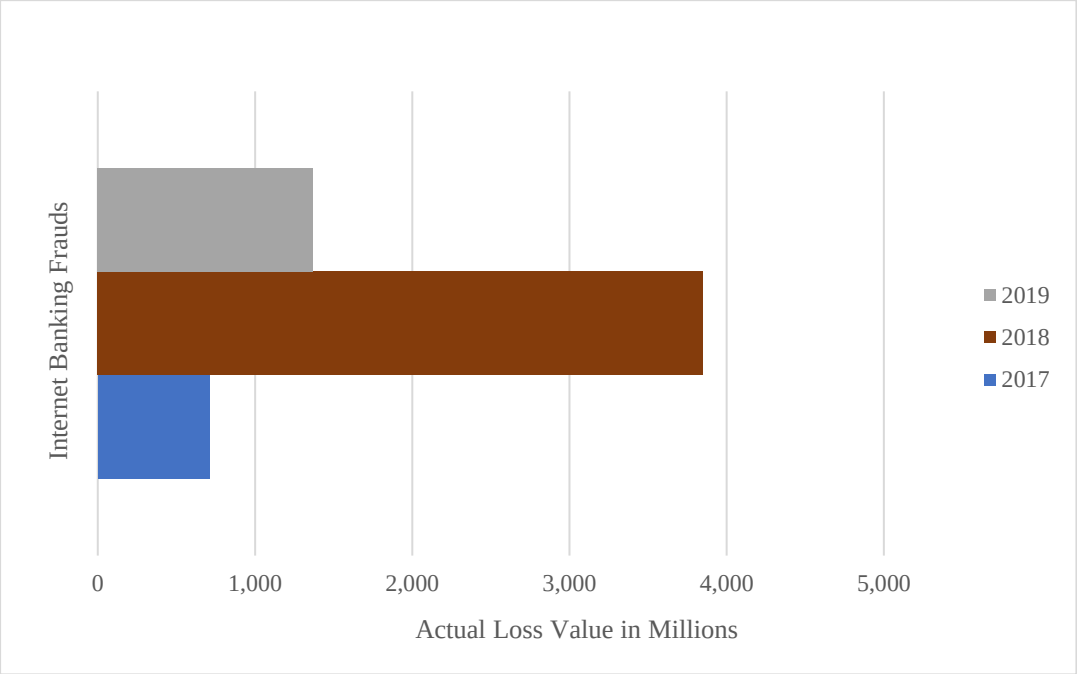

***Figure 6-2** Internet Banking Fraud Value in Nigeria Between 2017 - 19*[67]

As evidenced above, the actual fraud loss value recorded in the year 2018 for internet banking frauds was higher when compared with 2017. The 2017 figures were attributed to the prevailing unsuitable economic position of the country, increased unemployment rate amongst youth and insider abuse, while the 2018 losses were attributed to hacking, other cybercrimes and growing use of technologies.[68] Indeed, Hassan et al, confirm that unemployment, weak implementation of laws, poor enforcement capabilities and economic inequality are amongst the major causes of cybercrime in Nigeria.[69] The NFIU also echoes these concerns as it notes that key actors lack the required expertise on the mitigation of

[67] NDIC Annual Reports 2017 - 2019.
[68] NDIC, '2018 Annual Report and Statement of Accounts' 113 <https://ndic.gov.ng/wp-content/uploads/2019/09/NDIC-2018-ANNUAL-REPORT.pdf> accessed 4 September 2020.
[69] Anah Bijik Hassan, Funmi David Lass and Julius Makinde, 'Cybercrime in Nigeria: causes, effects and the way out' (2012) 2 Asian Research Publishing Network Journal of Science and Technology 626, 628 - 629.

cybercrimes, particularly, the inadequacy of resource and capabilities for law enforcement to effectively conduct cybercrime investigations.[70]

For the year 2019, losses recorded show a sharp decline from the previous year, attributed to enhanced cyber risk managements in banks.[71] However, we note that the value of losses in internet banking frauds remained the highest when compared against reported losses from 12 other channels.[72] More so, there is a possibility of information asymmetry due to inadequate investigation and monitoring as the NDIC in its quarterly report notes the lack of forensic hardware in tracing perpetrators and some evasion of cybercrime legislation by perpetrators.[73] Categories of fraud associated with temporary staff/third-parties accounted for the highest proportion which present a legal and management risk in terms of cybersecurity.[74] The use of third-party providers for banking services are unavoidable, hence it is important that FIs take steps to assess and monitor such providers, while ensuring that the services are provided with adequate security measures. This is important to prevent issues that arise with regards to data protection and privacy, organisational loss and liabilities.

6.4 The Self-Regulatory Fundamentals

Reflexivity in Organisational Requirements of Nigerian FIs

The case studies on four banking institutions carried out by Usman Kabir in 2016 focused on common risks encountered by FIs and provides an insight on the challenges to ensuring an effective cybersecurity risk management strategy.[75] In the study, strategies adopted by the banks show an integration of components of the risk management paradigms discussed in Chapter 3. The approach assesses the adopted measures by banks based off risks identified. For instance, adoption of Europay, Mastercard and Visa (EMV) chip cards to address card

[70] UNODC, 'NFIU Comment on Good Practices' 4.
[71] NDIC, '2019 Annual Report and Statement of Accounts' para 13.2.
[72] ibid Table 13.3.
[73] NDIC, 'The Impact of Cybercrime on The Nigerian Economy and Banking System' para 4.1.
[74] NDIC, '2018 Annual Report and Statement of Accounts' 117.
[75] Ahmad Kabir Usman, 'An investigation into the critical success factors for e-banking frauds prevention in Nigeria', University of Central Lancashire (2018) 140.

cloning issues takes into account the proportionality[76] feature of the risk-based approach through the implementation of measures proportionate to the risks.[77]

This section analyses the 2019 Annual Reports of Guaranty Trust Bank (GTBank) Plc and First Bank Plc which highlight technology/cyber risk as a major part of their broader risk scope. Similar to the previous chapters, findings from the reports are classified according to various risk management stages to aid assessment. While these findings may not represent sector-wide processes, they do give an idea as to the way in which banks are implement their cybersecurity resources.

The *GTBank Annual Report 2019* highlights technology risks as one of the key risks to its operations. The bank asserts its awareness of the value of data security and customer privacy noting that it implements "a robust legacy banking application and technology architecture that prevent data leakages and compromise".[78] However, information drawn from its reports are not as comprehensive as those from the other bank.

Risk Assessment Processes	Routine off-site and on-site assessments, carried out by the Group Information Security Assurance Team to evaluate the capabilities of existing information security infrastructures.[79] Utilises sophisticated tools to mitigate cyberattacks and ensure data security.
Risks Identified to Business Operations	Major risk areas include operational risks and technological risks, identified by designated risk personnel and Enterprise Risk Management (ERM)[80] and managed by ERM and relevant units.[81]

[76] R. Booth, G. Bastable and N. Yeo, *Money Laundering Law and Regulation: A Practical Guide* (OUP Oxford 2011) 208.
[77] Usman, 'An investigation into the critical success factors for e-banking frauds prevention in Nigeria' 147.
[78] Guaranty Trust Bank (GT Bank) Plc, '2019 Annual Report' 25 <https://www.gtbank.com/uploads/financial-information/2019-Annual-Report.pdf> accessed 16 September 2020.
[79] ibid.
[80] GT Bank Plc, '2019 Annual Report' 106.
[81] ibid 36.

Risk Control Frameworks	IT Risk Management Committee for introducing best IT risk management standards, enhancing IT risk management expertise, implementing cost-efficient solutions for managing technology risks and guaranteeing compliance.[82] Staff, customer and vendor awareness on security practices. Implementing international best practice such as the ISO 9001:2015 (Quality Management System), ISO 27001 (Information Security Management) etc. and compliance with the GDPR as well as other applicable regulations.[83]
Risk Review	Board Information Technology Strategy Committee who provide important advice to Board on IT concerns and reviews the adequacy, efficiency and effectiveness of IT controls.[84]

Table 6-1 *Risk management frameworks adopted by GTBank Plc*

Consistent with the earlier findings, the First Bank report finds that the increase in cybercrimes may be attributed to the growing use and anonymity of the internet, convenience of mobile channels, skills gaps and insufficient regulations.[85] The report also highlights significant developments in the bank's risk indicators comprising a 98.9% decrease in phishing email directed at customers and accelerated deletion of fake web pages and applications. Accordingly, it notes that the bank did not experience any major cyber-related breaches.[86] The classification of a cyber incident as major or not, is most likely dependent on policies created by the bank since the regulations are silent on such an issue. One consequence of that lack of an incident classification standard under regulation is an inaccurate level of reporting.

[82] ibid 22.
[83] GT Bank Plc, '2019 Annual Report' 31.
[84] ibid 15.
[85] First Bank of Nigeria Holdings (First Bank) Plc, '2019 Annual Report' 129 <https://www.fbnholdings.com/wp-content/uploads/2020/04/FBN_Holdings_Plc_2019_Annual_Report.pdf> accessed 16 September 2020.
[86] First Bank Plc, '2019 Annual Report' 145.

Risk Assessment Processes	Penetration testing, and other exercises to detect and fix possible vulnerabilities that can suspend operations.[87]
Risks Identified to Business Operations	Cybersecurity risks and threats for example, ransomware and targeted phishing attacks etc.[88] arising from failing IT systems and service outages.
Risk Control Frameworks	A 'three lines of defence' model: i) designated business units and other risk personnel, primarily responsible for detecting, quantifying, monitoring and managing risks, per their roles; ii) internal control systems monitoring, guidance and coordination created *via* several risk management strategies approved by the Board; and iii) evaluating and offering independent assurance on the effectiveness of the entire risk management frameworks, strategy and implementation.[89] An organisation-wide security awareness programme; and implementation of international best practices, including ISO 27001 and ISO 22301.[90] Compliance with relevant agency regulation on customer data privacy.
Risk Review	Continuous assessment of subcontracting arrangements; third-party security assessment of banks' systems and proactive security advise. Using verified risk assessment procedures that recommends the essential controls to lower risks to an acceptable level; taking record of the procedures; categorising IT assets according to risk priorities and allocating responsibilities.[91]

Table 6-2 *Risk management frameworks adopted by First Bank Nigeria Plc*

[87] ibid 120 - 121.
[88] ibid 119.
[89] First Bank Plc, '2019 Annual Report' 124.
[90] ibid 129.
[91] ibid 145.

Findings from both reports show the adoption of both reactive and proactive cybersecurity processes to monitor and detect existing risks, review the suitability of existing security controls and ensure compliance with relevant regulations.

Consistent with the UK and US reports, the risk assessment process adopted by the First Bank, echoes the reflexive law concept of learning, as through conducting threat scenario exercises, the bank is able to better understand and prevent against the possible risks to the availability of its services. Similar to the BofA's ERC function, the GTBank report highlights a form of shared understanding through collaboration between ERM and relevant units in managing risks identified i.e. governance of the risk discourse through reflexive interactions. Also, while both reports do both specifically mention third-party risks as with the UK and US case, the presence of this is observed through reference to vendor cybersecurity practice awareness, sub-contracting arrangements and third-party security assessments.

Both reports also suggest that the importance of designating relevant personnel to oversee cybersecurity policy decision, monitor cyber risk profiles and ensure effectiveness in implementation, a function that seems absent in many regulatory systems. In addition, findings from the First Bank report employ the concept of risk prioritisation, a part of risk management which entails the proportionate apportionment of resources to risks identified. In contrast with the UK and US, both annual reports, however, make no mention of coordination with law enforcement and regulators, thus echoing earlier concerns of law enforcement inadequacies.

In summary, both reports suggest the progressive attitudes of banks towards strengthening cybersecurity resilience, but also imply the need for banks to focus on collaboration with law enforcement and other key actors.

6.5 Reflexivity in Regulation and Supervision

Guidelines which make provisions for privacy, data protections and the detection, mitigation, monitoring and prevention of cybersecurity incidents are contained in publications issued by the CBN to assist with the regulation of payment platforms and services which could be at risk of online fraud or other cybercrimes namely: the regulatory framework for mobile

payment services (MPS) in Nigeria[92], guidelines on Mobile Money Services (MMS) in Nigeria[93], Guidelines on operations of electronic payment channels in Nigeria[94], the regulatory framework for the use of Unstructured Supplementary Service Data (USSD) in the Nigerian Financial System[95], the regulatory framework for Bank Verification Number (BVN) operations and watch-list for the Nigerian financial system[96], the Nigerian payments system risk and information security management framework[97] and the risk-based cybersecurity framework and guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs).

In this chapter, however, we would only be discussing the *Risk-Based Cybersecurity Framework* for DMBs and PSPs. Generally, the guideline requires the use of assessment in developing risk management plans and estimating resources i.e. decision-making based off observation. In addition, it ensures that actors take into proper consideration all possible information on evolving threats, risks, cyberattacks, instruments and potential causes of attacks.[98] This thought process and information trading, hinges on the notion of reflexivity, which ultimately steers learning.

The guidelines were issued by the CBN as a response to the ever-increasing cyber threat and risk landscape to ensure the safety and soundness of the institutions which it regulates. These guidelines, though condensed, identify major cybersecurity issues

---

[92] CBN, 'The Regulatory Framework for Mobile Payment Services in Nigeria' (November 2014) <https://www.cbn.gov.ng/out/2014/bpsd/exposure%20draft%20regulatory%20framework%20for%20mobile%20payments%20.pdf> accessed 10 March 2019.
[93] CBN, 'Guidelines on Mobile Money Services' (June 2015) <https://www.cbn.gov.ng/out/2015/bpsd/guidelines%20on%20mobile%20money%20services%20in%20nigeria.pdf> accessed 10 March 2019.
[94] CBN, 'Guidelines on operations of electronic payment channels in Nigeria' (April 2016) <https://www.cbn.gov.ng/Out/2016/BPSD/Approved%20Guidelines%20on%20Operations%20of%20Electronic%20Payment%20Channels%20in%20Nigeria.pdf> accessed 12 March 2019.
[95] CBN, 'The regulatory framework for the use of unstructured supplementary service data (USSD) in the Nigerian Financial System' (April 2018) <https://www.cbn.gov.ng/Out/2018/BPSD/USSD%20Regulatory%20Framework.pdf> accessed 12 March 2019.
[96] CBN, 'The regulatory framework for Bank Verification Number (BVN) operations and watch-list for the Nigerian financial system' (October 2017) <https://www.cbn.gov.ng/out/2017/bpsd/circular%20on%20the%20regulatory%20framework%20for%20bvn%20%20watchlist%20for%20nigerian%20financial%20system.pdf> accessed 12 March 2019.
[97] CBN 'Exposure draft of the Nigerian payments system risk and information security management framework' (May 2018) <https://www.cbn.gov.ng/Out/2018/BPSD/NPS_Risk_and_Info_Sec_Mgt_Framework.pdf> accessed 12 March 2019.
[98] CBN, 'Risk-Based Cybersecurity Framework and Guidelines for DMBs and PSPs' para 3.9.1.

highlighted in the reports of other jurisdictions which already have regulations, policy and guidelines covering most issues of relevance to cybersecurity. For instance, in the USA, the FFIEC's *2017 Annual Report* notes that 'risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incident management and resilience' are crucial cybersecurity areas.[99] Likewise, the UK's FCA in its *Business Plan 2019/20* stresses its focus on assessing third-party arrangements, responding to major cyber incidents or disruptions through coordination with other relevant authorities and regulations, CBEST for testing resilience and supervisory firm-wide engagement to properly understand institutions' vulnerabilities in identifying their key assets, detecting cyberattacks and enhancing resilience.[100] For this reason, the Financial Stability Board (FSB),[101] in its *Summary Report* observed that regulations and guidance which address cybersecurity risks should cover elements such as governance; risk assessment and management; role of the board; responsibilities of the chief information security officer; information sharing; regulatory reporting; and auditing.[102]

This framework, allowing DMBs and PSPs to construct their risk management models and mitigate threats, subject to their accountability to the CBN, is characterised by reflexivity which draws upon actions to produce and reproduce knowledge, that produces and reproduces actions to ensure consistency and effectiveness in regulation. A similar approach can be seen to be taken by the US mandating FIs to share cyber threat and prevention information with regulators.[103] The UK, on the other hand, though having an overarching NIS Regulation providing for operators of essential services, fails to enforce its applicability in the financial services sector.[104] Although, FIs are still able to share information through

[99] FFIEC, 'Annual Report 2017' (30 March 2018) 27 <https://www.ffiec.gov/PDF/annrpt17.pdf> accessed 14 March 2019.
[100] Financial Conduct Authority, 'Business Plan 2019/2020' 17 <https://www.fca.org.uk/publication/business-plans/business-plan-2019-20.pdf> accessed 5 January 2020.
[101] An international organisation in charge of monitoring, examining financial stability and offering proposals for the global financial system.
[102] FSB, 'Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices' (13 October 2017) 4 <http://www.fsb.org/wp-content/uploads/P131017-1.pdf> accessed 14 March 2019.
[103] Cybersecurity Information Security Act 2015, Section 104 (C)(1).
[104] NIS Regulations 2018, Section 10.

regulatory guidelines.[105] The CBNs Risk-Based Cybersecurity Framework is summarised in the table below:

Cybersecurity Governance and Oversight[106]	• sets out the roles and responsibilities of the Board, Management, Compliance department, CISO etc. • cybersecurity strategy implementation, day-to-day monitoring of cybersecurity operations and ensuring compliance to relevant policies or regulations • carry out background checks on staff who implement security policy frameworks and process.
Cybersecurity Risk Management System[107]	• covers the processes by which DMBs and PSPs may integrate cyber-risk management as part of their institutional strategies. • activities include an up-to-date and timely risk assessment; risk measurement; risk mitigation/risk treatment and risk monitoring and reporting. • result of resilience assessments to be used in risk management planning.
Cybersecurity Operational Resilience[108]	• requires DMBs and PSPs to develop, promote and maintain a resilient cybersecurity operational strategy. • to establish two minimum controls to guarantee that information assets are protected up to Know Your Business[109] Confidentiality, Integrity and Availability standards. • a Cyber Threat Intelligence policy for the purpose of identifying new forms, patterns and trends of cyber threats/risks and potential impacts.
	• requires DMBs and PSPs to establish metrics and monitoring strategies to ensure compliance and inform the basis for suitable management decisions.

[105] FCA Handbook, Principle 11, and SUP 15.3.
[106] CBN, 'Risk-Based Cybersecurity Framework and Guidelines for DMBs and PSPs' para 2.
[107] ibid para 3.
[108] ibid para 4.
[109] This involves being aware of the business environment and critical assets and implementing mechanisms to ensure an up-to-date log of authorised programmes, applications, network devices or other IT-related functions to ensure timely identification, assessment and response to any threats, risks, and vulnerabilities.

Metrics, Monitoring & Reporting[110]	• metrics should involve an evaluation of the effectiveness of DMBs and PSPs overall cybersecurity programme and a measurement of its performance using tools such as key risk indicators, key success factors, etc.

Table 6-3 *CBN Risk-Based Cybersecurity Framework and Guidelines*

A failure to comply with any of these guidelines may attract relevant sanctions by the CBN in line with the provisions of the BOFIA 1991 and CBN Act 2007.[111] The current guideline at its present state is quite comprehensive and capable of providing a good starting point for effective cybersecurity regulation. Although, there is no evidence as yet to support its implementation. Challenges to the operationalisation of the regulatory framework may be attributed to issues relating to the interdependence of regulatory structures which Black[112] regards as the key feature of autopoietic systems. In order for the decentred approach to be an effective alternative to the command-and-control approach, there needs to be collaboration between regulatory, law enforcement agencies and FIs, and systems of accountability in place to produce learning, coordination and knowledge that helps develop systems of accountability.

The guidelines are very similar to those issued by the FFIEC in its Handbook and CAT for financial institutions.[113] In fact, the guidelines list the FFIEC and US-CERT as its first two cybersecurity self-assessment tools to be considered.[114] While it is often commonplace for developing countries to follow models of developed countries in creating their laws, it is important to conduct an appraisal prior to its adoption, of whether these frameworks are institutionally suitable and whether it has the capabilities required for its implementation.

[110] CBN, 'Risk-Based Cybersecurity Framework and Guidelines for DMBs and PSPs' para 5.
[111] ibid para 6.3.
[112] Black, 'Critical reflections on regulation' 28.
[113] Namely Risk management and oversight, Threat intelligence and Collaboration, Cybersecurity controls, External dependency management and Cyber incident management and resilience.
[114] CBN, 'Risk-Based Cybersecurity Framework and Guidelines for DMBs and PSPs' Appendix II.

Compared to its draft guidelines which supplies empty links to the CBNs homepage for threats and incidents reporting templates,[115] the final guidelines provide comprehensive templates which take into account risk levels, impacts and controls. Although, it is argued that though the maintenance of these guidelines appear preventive and corrective, they are barely instructive on the basis of our argument in Section 3.8. In this regard, we observe that while there are some provisions for supervision, intervention and issuance of fines in the event of non-compliance, the set guidelines do not include maturity levels[116] within the context of the assessment. Instead, it merely notes that enhancing cybersecurity resilience is necessary for increasing cybersecurity maturity levels[117] without specifying nor defining the various maturity levels, which are necessary for assessing the practices of FIs as they progress from the lowest to the highest level i.e. baseline to innovative. Moreover, the regulatory framework appears fixated on rule-setting with minimal focus on the structures that need to be present for their implementation. This echoes our argument in Chapter 3 that in the absence of well-defined functions, learning may not inform attainment of objectives, and is further reinforced by Markandya who note that "Existing regulations, in developing countries are usually replicas of past regulations in developed countries . . . [which are barely founded] in local realities and cultures and therefore are largely unenforceable".[118]

Importantly, the rationale for using the USA model can only be compelling if there is a similarity in cybercrimes, where resources/capability position is adequate and where enforceability is given priority. Where any such variables are absent, it would appear that Nigeria must seek a different approach to implementation. In this case, cybercrimes involving money transfer scams and insider abuse appear to be more prominent in the Nigerian case than in the UK and US, not to mention issues of inadequate resources and infrastructure, substandard compliance with cybercrime laws by FIs, ill-equipped law enforcement and weak

[115] CBN, 'Exposure draft of the risk-based cybersecurity framework and guidelines for deposit money banks and payment service providers' (June 2018) Appendix I <https://www.cbn.gov.ng/Out/2018/BSD/RISK%20BASED%20CYBERSECURITY%20FRAMEWORK%20Exposure%20Draft%20June.pdf> accessed 14 March 2019.
[116] The maturity level involves a list of indicators that illustrate how the conducts, approaches, and procedures of FIs can 'consistently' generate desired results, complements the risk management process, and helps to ascertain whether relevant levels are appropriate to risks identified. FFIEC, 'Cybersecurity Assessment Tool' (May 2017) 2 <ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf> accessed 18 August 2018.
[117] CBN, 'Risk-Based Cybersecurity Framework and Guidelines for DMBs and PSPs' para 4.2.
[118] A. Markandya and Food and Agriculture Organization of the United Nations, *Policies for Sustainable Development: Four Essays* (Food and Agriculture Organization of the United Nations 1994) 219.

penalties for cybersecurity breaches.[119] In view of this, if the threats needed to be addressed are almost completely different and the mechanisms in place, deficient, then the responses proposed will be inherently different and may thus make replication, to a significant extent, pointless. This is particularly the case where texts are being transposed without much consideration of practice. If developed country models were assessed before adoption by developing countries, challenges to clarity, enforceability, practicability, efficiency and effectiveness may be exposed and solutions may be found.

The 'Regulatory Co-Existence' Hypothesis

There is very little empirical evidence supporting this hypothesis in the Nigerian case, not because there has been no enforcements at all, but because cybercrime related enforcements have been directed at individuals and not FIs. However, the absence of such information does not automatically render the hypothesis invalid. In fact, a number of individual cases have shown the EFCC's willingness to prosecute cybercrimes.[120] Given this, we proceed to the next sections to access the applicability of regulations, and ultimately, possible challenges to the reflexivity of regulation which render the applicability of regulation, impractical, in FIs.

6.6 Criminal Justice Responses Applicable to Nigerian FIs Under Legislation

International Response to Cybercrime

Budapest Convention on Cybercrime

In the earlier chapters, we mentioned that the Budapest Convention is the only international non-legally binding instrument which addresses issues of cybercrime. As far as Nigeria is concerned, it is yet to sign or ratify the convention. However, it has on several occasions collaborated with the COE regarding cybercrime issues. In search of ways to effectively combat the threat of cybercrime, Nigeria wrote a letter of request the COE for an invitation to

[119] Victoria Wang, Harrison Nnaji and Jeyong Jung, 'Internet banking in Nigeria: Cyber security breaches, practices and capability' (2020) 62 International Journal of Law, Crime and Justice 100415, para 5.3.
[120] Economic and Financial Crimes Commission, 'EFCC Arrests Three Suspected Fraudsters for Attempted Hacking' <https://efccnigeria.org/efcc/news/987-efcc-arrests-three-suspected-fraudsters-for-attempted-hacking> and 'N466m Fraud: Fraudsters who Defrauded Polaris Bank Get N1m Bail' <https://efccnigeria.org/efcc/news/3659-n466m-fraud-fraudsters-who-defrauded-polaris-bank-get-n1m-bail> accessed 24 September 2020.

accede. In response, the COE at its 1291st meeting on the 5th of July 2017 had sent Nigeria an invitation to accede.[121] Therefore, if Nigeria accedes to the convention, it will be able to benefit from the co-operation between countries to combat evolving threats and also be required to criminalise substantive criminal law conducts as well as implement procedural instruments useful for the investigation and prosecution of cybercrimes.

Domestic Legislation/Regulation relating to Cybersecurity for FIs

Existing laws and regulations criminalising cyber-related crimes in Nigeria include the Advance fee Fraud and other Fraud Related Offences Act 2006, Cybercrimes Act 2015, EFCC Act 2004, Evidence Act 2011, Money Laundering Prohibition Act 2011 and Nigerian Data Protection Regulations (NDPR) 2019. However, the relevant laws containing cybersecurity requirements and standards for FIs are set forth in the table below.

Cybercrimes Act 2015	• criminalises the offences of hacking, DDoS, phishing, malware, and identity theft. • Section 19(3) provides for duties of FIs to establish effective measures for the prevention of cybercrime.
NDPR 2019	• mirrors the EU's GDPR and covers the privacy and protection of data. • provides a requirement for data controllers (in this case, FIs) to ensure appropriate measures are taken in processing the information of data subjects (in this case, customers);[122] • provides for designation of a data protection officer[123] and for violation of provisions.

Table 6-4 *Nigerian Laws Specifying Cybersecurity Best Practices*

Cybercrimes Act 2015

[121] Council of Europe, 'Convention on Cybercrime (ETS No. 185) - Request by Nigeria to be invited to accede' <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680717468> accessed 15 March 2019.
[122] Nigerian Data Protection Regulations (NDPR) 2019, Article 2.13(1).
[123] NDPR 2019, Article 3.1(2).

The 2015 Act sought to implement changes to a number of issues bordering on the security of financial transactions, security of sensitive information, reporting cyber incidents, role of relevant agencies in mitigating cyber threats, among others. While some of its provisions are already being implemented to aid in the achievements of its objectives, there have been others whose implementation appear to defeat some of its objectives.

First, the Act provides for the offence of hacking, committed through "intentional access without authorisation, whole or part of a computer system or network for fraudulent purposes and obtains data crucial to national security or if they intend to obtain computer data, secure access to any program, classified information or commercial or industrial secrets".[124] This section has been argued to be inevitably limited in application to the question of the significance of fraudulent purpose/intention (to obtain computer data, secure access to any program, commercial or industrial secrets or classified information). Omotubora notes that it provides an escape route for hacking offences, for instance, in the event where a hacker performs unauthorised access to a bank's computer system, they may escape liability under the Act if they are able to successfully argue that their conduct was without fraudulent intent.[125]

The Act limits the forms of data which may be hacked and fails to identify what amounts to 'classified information'.[126] It further stipulates a fine of not more than N7, 000,000.00[127]or a three-year imprisonment as a maximum sentence, or both. The meagre fine involved may trigger lax attitudes to compliance. A recent study on Nigerian banks by Tayo-Tiwo evidenced this problem and suggest that fines prescribed in the legislation encourages low compliance and that smaller fines equal less compliance because due to the meagre sum of the fines, most FIs favored taking risks and paying fines, other than obeying the law.[128] This finding is validated by results from the study conducted by Yusuf on the implications of penalties issued by regulators on the operations of Nigerian banks which reveal that penalties

[124] Cybercrimes Act 2015, section 6 (1).
[125] Adekemi Olufunmilola Omotubora, 'Comparative perspectives on cybercrime legislation in Nigeria and the UK - a case for revisiting the "hacking" offences under the Nigerian Cybercrime Act 2015' (2016) 7 European Journal of Law and Technology 1, 6.
[126] ibid 5.
[127] About £11,667.
[128] Aderonke Alberta Tayo-Tiwo, 'Nigerian Banks' Compliance with the Code of Corporate Governance', Walden University (2018) 142.

issued for non-compliance with regulations and CBN guidelines such as the Corporate Governance Code, Anti-Money Laundering and Know Your Customer framework, have no material effect and are regarded as operational costs.[129] These findings, indicate the continuous existence of the enforcement challenges in the sector highlighted by Nigeria's former Central Bank President.

While there is no one-size-fits-all model when it comes to setting fines and penalties, a rational approach would be to set fines and penalties at a level proportionate to the violation. Other extreme measures such as stipulating a higher sum or withdrawing their service licence may also be more effective considering that the goal is to deter FIs and service providers who may attempt to provide services without implementing appropriate security measures. Nevertheless, weak law enforcement may present challenges to the detection and punishment of cybercrimes.

Next, the provision of Section 19(3) of the Act appears to be highly problematic. It states that:

> "Financial institutions must as a duty to their customers put in place effective counter fraud measures to safeguard their sensitive information, where a security breach occurs the proof of negligence lies on the customer to prove the financial institution in question could have done more to safeguard its information integrity".

The language of section 19(3) of the Cybercrimes Act: "FIs must as a duty to their customers put in place effective counter fraud measures to safeguard their sensitive information", show the intention of the lawmakers to establish a duty on FIs with regards to the prevention of fraud and security of customer information. However, the words "where a security breach occurs the proof of negligence lies on the customer to prove the FI in question could have done more to safeguard its information integrity" may be interpreted as the court placing the onus of proof on the consumer to disprove that they have been negligent and establish that it was in fact, negligence on the part of the FI. This is an unfair consumer practice which has

[129] Data collected from 15 deposit money banks in Nigeria between the years 2006 to 2015; Ismaila Yusuf and Damola Ekundayo, 'Regulatory non-compliance and performance of deposit money banks in Nigeria' (2018) 26 Journal of Financial Regulation and Compliance 425, 436 – 437.

been argued to defeat the 'consumer protection objective' as it fails to place the FI in a position of responsibility for greater liability, considering that it is the stronger party.[130] This has also been argued to breach the requirement of implied fiduciary obligation of secrecy and confidentiality[131] owed by FIs to consumers who would reasonably expect a safeguard of their information.[132]

In the UK and US, an entirely different approach has been taken, in favour of consumers. In the UK, there are frameworks in place to ensure that customers who are genuine fraud victims receive a timely refund and suffer no loss. Complying with Regulation 72 of Directive (EU) 2015/2366 of the European Parliament on Payment Services in the Internal Market Regulation, Regulation 75(4) of the UK's PSR 2017 that "if a payment service provider, including a payment initiation service provider where appropriate, claims that a payer acted fraudulently or failed with intent or gross negligence to comply with Regulation 72, the payment service provider must provide supporting evidence to the payer". The US also takes a similar approach on the issue of unauthorised funds transfer, placing the burden of proof upon the FI to establish liability conditions, and in other cases limiting liability subject to the FI establishing negligence on the part of the consumer to make a report which could have prevented further losses, in accordance with the Payment Systems and Electronic Fund Transfers Act 2007, Section 1693g(b).

Given the weaker liability for FIs in Nigeria, motivations for preventing such risk would be reduced and it may thus be more likely for cybercriminals to exploit the gap to perpetrate fraud. The banking system is inherently founded upon trust[133] and as such, any framework which seeks to violate the protection of consumers may result in reduced adoption of e-banking services and adverse effects for the financial system. Meanwhile, such issues may be in part due to the fact that at the time of adoption, the country had not enacted any comprehensive privacy and/or data protection legislation which may effectively help with

[130] Uchenna Jerome Orji, 'Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria' (2019) 24 Tilburg Law Review 105, 113.
[131] ibid 113.
[132] J. O'Donovan, *Lender Liability* (Sweet & Maxwell 2005) 180.
[133] B. Christiansen and A. Piekarz, *Global Cyber Security Labor Shortage and International Business Risk* (IGI Global 2018) 49.

reinforcing the rights of consumers with regards to how their personal/sensitive data is being managed.

Similar concerns were also observed in a case study of Nigerian banks conducted by Okpara et al who found that the legal protection for customers was hypothetical, exist only in the books and at the very least weak. In the study, for example, a deputy general manager in one of the banks confirmed that "if a customer experiences identity theft in the course of using an online service, everything is pushed to them as consumer protection is in fact non-existent".[134]

The UK and US regime has maintained the objective of protecting consumers and ensuring the accountability of FIs. The importance of learning from such regimes is that it will serve as a deterrence for FIs in Nigeria who do not have up-to-date and effective frameworks in place for monitoring fraudulent activities in its systems.

NDPR 2019

The NDPR issued by the National Information Technology Development Agency (NITDA), appears to be an aspiring model of the GDPR. However, it does not adapt the very significant provisions of the GDPR. While the GDPR offers a wide extraterritorial scope for the processing activities of data controllers and processors without presence in the EU, but with associated operations involving the EU and persons in the EU[135], the extraterritorial scope of the NDPR is limited only to Nigerian citizens residing outside Nigeria.[136] In contrast to the GDPR special categories of personal data, the NDPR defines sensitive personal data to include "any other sensitive personal information",[137] which may include financial data. Although, unlike the GDPR,[138] it makes no specific provisions for the processing of such data. Also, compared to the GDPR which places explicit record-keeping requirement of processing activities on data controllers or processors,[139] the NDPR makes no such provision

[134] Okpara, 'Bank reforms and the performance of the Nigerian banking sector: An empirical analysis' 240.
[135] GDPR, Article 3.
[136] NDPR 2019, Article 1.2 (b).
[137] NDPR 2019, Article 1.3 (v).
[138] GDPR, Article 9.
[139] GDPR, Article 30.

and may therefore raise accountability issues or present challenges to an investigation where detailed records are needed.

In addition, the GDPR requires a data breach notification by the data processor to the controller without undue delay,[140] whereas the NDPR makes no provision on this, thus failing to take into account third-party cybersecurity risks. Where an organisation dealing with over 10,000 data subjects breaches the NDPR, it can be fined up to 2% of an its annual gross revenue of the preceding fiscal year, or payment of N10 million[141], whichever is higher.[142] Meanwhile, under the GDPR, an organisation can be fined up to 4% of its annual global revenue.

While the NDPR provides a good starting point for regulating issues surrounding personal data protection, a draft Data Protection Bill 2020 is being considered by the Nigerian Senate which would, if enacted, provide more comprehensive and specific rules regarding personal and sensitive data processing activities, data subject rights and other related issues. Compared to the NDPR which only provides an obligation for institutions to carry out an audit of data privacy and protection processes[143], under the proposed bill, there is a stipulated 48-hour deadline for data controllers to notify data subjects of a breach, following notification to the Data Protection Commission (DPC).[144] Although, there is no clarity as to the timeframe for the notification of the data breach by the controller to the DPC. On the function of personal data processing by the data controller, the Bill uses a language consistent with security provisions in both the NIS Regulations and GDPR, requiring proportionality[145] and appropriateness of technical and organisational methods, respectively. Although, merely adopting a wording or more from these legislations will not translate to learning that is acquired from repeated practices, which are central to implementation.

The Bill sets a minimum fine of N10 million[146] yearly, for as long as the violation continues or an imprisonment term of at least a year or both. Compared with the fines for data

[140] GDPR, Article 33(2).
[141] About £16,666.
[142] NDPR 2019, Article 2.10.
[143] NDPR 2019, Article 4.1 (5)(i).
[144] Data Protection Bill 2020, Section 17(3).
[145] Data Protection Bill 2020, Section 30 1(a) - (b).
[146] Approximately £16,667.

protection violations under the UK DPA set at a maximum of £17 million or 4% of organisation's annual turnover, and enforcement powers given to authorities in the US to impose fines costing organisations millions of their profits, the penalties under the NDPR and this Bill appears to have been set too low, that it may arguably have any effect. While the effect of a yearly fine may be considered substantial in terms of its cumulative effect, it is argued that the deterrent effect will be inadequate, such that it may not achieve the effective, proportionate, and dissuasive objective, specified under Article 83 of the GDPR and Section 155(3)(l) of the DPA 2018.

The Bill also creates the DPC organisation[147] and a Commissioner[148], an equivalent of the UK's ICO. For the DPC, it sets out a Board consisting of the Commissioner and a Director or equivalent representative each from 11 listed government agencies and institutions., some of which include the CBN, Police Force, Electoral Commission, Immigration Service and Road Safety Commission.[149] This board composition appears problematic and may result in governance and conflict of interest issues as the members are drawn from the leadership of government institutions, most of which are under increased government influence. In contrast, the UK's ICO is characterised by a high level of independence with a Management Board consisting of the Commissioner, a Deputy CEO and three other Deputy Commissioners each with strategic and relevant functions relating to corporate strategy and planning, regulatory investigation and supervision, stakeholder liaison and global strategy, and guidance and research on technology and innovation policies and agendas.[150] It therefore becomes important that the DPC's Board is restructured.

Given that, it is recommended that the members of Board do not include any of the listed government agencies, but may more appropriately include departments established by the DPC for the effective execution of its functions, in accordance with Section 7(3). This is because implementation of the provision may place the DPC under the influence of specified institutions and political interference, thereby infringing its requirement to act in full

[147] Data Protection Bill 2020, Section 7 (1).
[148] Data Protection Bill 2020, Section 11.
[149] Data Protection Bill 2020, Section 8(1).
[150] Information Commissioner's Office, 'Management Board' <https://ico.org.uk/about-the-ico/who-we-are/management-board/> accessed 19 January 2021.

autonomy and neutrality in carrying out its functions and the exercise of its powers[151] Likewise, in recognition of the regulatory/statutory public functions performed by the listed institutions for the law enforcement purposes, it is proposed that they are instead regarded as competent authorities governed by a law enforcement processing regime, in line with Part 3 and Schedule 7 of the UK's DPA 2018.

In summary, while the introduction of the Cybercrimes Act 2015 and the NDPR may be regarded as a laudable step by the Nigerian legislature, some of its provisions appear to have been drafted without seemingly being informed by reflection. Equally important, the Data Protection Bill 2020, needs to be refined to address cybersecurity risk realities and uncertainties, involving data as well as the networks and systems by which they are processed. Awhefeada et al make a case for introducing state-specific cybercrime laws similar to the US, arguing that cybersecurity should be a decentralised responsibility between state and federal government and that Canada as well, designates several government divisions with the prevention of cybercrime.[152] While such argument may be perhaps tenable in countries with well-developed legal systems and economies, it is less tenable in Nigeria where its developing legislative and judicial arm of government is an already unstable system, owing to corruption and political connections which affect the clarity and independence of authorities in enforcement. More so, if such an argument were plausible, it would further place Nigeria in a position of increased confusion arising out of inconsistencies in its laws and regulatory structures.

On the whole, we have observed from the Nigerian case that the existing laws and institutions have not worked mainly due to passive enforcement and duplication of responsibilities. Thus, a suggested starting point would be a gradual reshaping and balancing of its enforcement strategy, adapting applicable practices to inform effective implementation as the system learns from experiences.

[151] Data Protection Bill 2020, Section 9(f).
[152]Awhefeada and Bernice, 'Appraising the Laws Governing the Control of Cybercrime in Nigeria' 47.

6.7 Possible Challenges to Reflexivity in Nigeria FI Cybersecurity Regulation

Like the UK and US, challenges to reflexivity in Nigeria's financial sector cybersecurity regulation include inadequate cyber incident disclosures, conflicting institutional mandates and no uniform standard for data privacy and protection, some of which have been discussed earlier. More importantly, the challenges faced in the Nigerian system is significantly different as the cause of many of these issues hinges on its governance structures.

Therefore, in this section, we consider some of the factors highlighted by the former CBN President, as contributing to the failure of the Nigerian banking system during the period of the global financial crisis which are still prevalent, even after almost a decade.[153] These factors, which threaten the success of reflexive cybersecurity practices in Nigerian FIs include inadequate regulatory frameworks, corporate governance deficiencies, unclear structures for information sharing, uneven supervision and enforcement and political interference.

Corporate Governance Deficiencies

Using Stirling's mirror analogy,[154] Weiland and Feindt note a jointly dependent relationship between governance and reflexivity, where reflexive learning informs the formation and transformation of governance structures and where governance in turn dynamically drives reflexivity.[155] As such, it may be argued that there is a causal relationship between corporate governance and reflexive cybersecurity practices, in that effective and up-to-date corporate governance practices will ensure that cybersecurity frameworks, structures and policies are married with effective implementation throughout the institution. However, there is a problem with conceiving such links in the Nigerian system due to political, social, and cultural influences.

Corporate and cybersecurity governance failures in Nigerian FIs may be regarded as key factors, contributing to the ineffectiveness of its cybersecurity regulatory framework. In

[153] Sanusi, 'The Nigerian Banking Industry: what went wrong and the way forward' 3.
[154] Andy Stirling, 'Precaution, foresight and sustainability. Reflection and reflexivity in the governance of science and technology' (2006) Reflexive governance for sustainable development Cheltenham: Elgar 225, 227.
[155] Peter H. Feindt and Sabine Weiland, 'Reflexive governance: exploring the concept and assessing its critical potential for sustainable development. Introduction to the special issue' (2018) 20 Journal of Environmental Policy & Planning 661, 670.

Nigeria, factors which undermine its corporate governance effectiveness include corruption and patronage systems,[156] lack of a set emergency response plan for cybersecurity incidents, accidental damage or destruction of data and IT systems as a result of human input/non-input causes, inadequate staff training, compromise of customer banking data by third party providers, insider abuse and fraudulent enrichment of staff or operators of the institution at the expense of the institution or its clients.[157] The ownership structure of banks have also been found to affect governance structure where owners take advantage of their position to embezzle institutional funds[158] or plunder depositors' funds.[159] Meanwhile, banks as well as the EFCC have been found to face challenges in relation to staff recruitment training.[160] Fields observes that even in instances where cybersecurity training had been provided, Nigerian banks failed to monitor staff compliance to IT policies.[161]

Kshetri argues that major African countries regard cybersecurity as a luxury, particularly noting that public officials in Nigeria were reported to have maintained unawareness of the cybercrimes in the country, describing it as 'Western propaganda'.[162] A recent pilot study evaluating the compliance of 18 banks carried out by the CBN in March 2017 highlights this unawareness of FIs to the importance of adopting effective risk management processes as part of its corporate governance functions. Some findings from the study revealed the following: failure by some banks' to adhere to corporate governance code requirements on board composition and risk management, lack of a detailed and effective approved strategy document, and failure to delegate tasks for the implementation of approved strategy document.[163] The findings of this study also confirms Soludo's contention that effective regulation is greatly influenced by strong corporate governance structures. Further, it

[156] F.N. Ngwu, O.K. Osuji and F.H. Stephen, *Corporate Governance in Developing and Emerging Markets* (Taylor & Francis 2016) 261.
[157] Munirul Ula, Zuraini Ismail and Zailani Mohamed Sidek, 'A Framework for the governance of information security in banking system' (2011) 2011 Journal of Information Assurance & Cyber Security 1, 3.
[158] Masrur Reaz and Thankom Arun, 'Corporate governance in developing economies: perspective from the banking sector in Bangladesh' (2006) 7 Journal of Banking Regulation 94, 108.
[159] GMT Emezue, Inge Kosch and Maurice Kangel, *Justice and Human Dignity in Africa* (Lulu 2014) 280.
[160] Umar, Samsudin and Mohamed, 'Ascertaining the effectiveness of Economic and Financial Crimes Commission (EFCC) in tackling corruptions in Nigeria' 664.
[161] Z. Fields, *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution* (IGI Global 2018) 222.
[162] Kshetri, *Cybercrime and Cybersecurity in the Global South*, 78.
[163] CBN, 'Central Bank of Nigeria Annual Report 2017' 58 <https://www.cbn.gov.ng/Out/2018/RSD/CBN%202017%20ANNUAL%20REPORT_WEB.pdf> accessed 10 March 2019.

shows that regulatory assessments are especially important for identifying weaknesses in corporate governance practices which may blur the lines of accountability, adversely affect the FIs cybersecurity decision making process and consequently, present challenges to the effective implementation of risk management frameworks.

Unclear Structures for Information Sharing

Some of the authorities saddled with the regulation of the financial sector often lack oversight resulting from uncoordinated information sharing among regulators, thereby preventing the CBN from gaining a comprehensive outlook of FIs' operations. In spite of the many cyber-related laws and cybersecurity guidelines, there are no well-established standards implemented for sharing information on cyber incidents between financial regulators at national level. As discussed earlier, regulations governing cybersecurity in Nigeria's financial sector are yet to fully progress to the implementation stage. More so, with many of these regulations in need of adjustments. Conversely, in the UK and US, the culture of information sharing in FIs is enhanced through clearer guidelines on cyber incident reporting to regulators as well as initiatives like the CiSP and FS-ISAC, established to co-ordinate information sharing among financial communities and respond to extensively evolving forms of threats, respectively.

In its quarterly report, the NDIC notes initiatives between the financial sector, IT experts and a pilot programme of the Nigerian Computer Emergency Response Team (NG-CERT).[164] It, however, fails to explain what these initiatives are and how they specifically facilitate the sector's cybersecurity objectives. Moreover, the NG-CERT's authority to co-ordinate cyber security incident response and mitigation plans suffers from an overlap of functions between it and other government agencies as well as information asymmetries between relevant institutions at national level. The NG-CERT's introduction in 2015 seemed to be a significant change, however, its achievements are not yet visible. Of the 18 advisories published in the six years of its establishment, there is none specifically related to the financial sector.[165] It also documents news on cybersecurity using RSS feeds from *Threatpost*,

[164] NDIC, 'The Impact of Cybercrime on The Nigerian Economy and Banking System' para 6.2.
[165] Nigerian Computer Emergency Response Team, 'Advisories' <https://www.cert.gov.ng/advisories> accessed 19 September 2019.

an independent online information source for cybersecurity, but fails to provide specific reports on cybersecurity incidents related to Nigeria.

By virtue of Section 21 of the Cybercrimes Act 2015, the NG-CERT is to receive cyberattack reports, create a shared incident awareness platform, coordinate information sharing amongst institutions. However, this authority to receive reports is also exercised by the EFCC in accordance with its powers under the EFCC Act. Likewise, the CBNs Risk-Based Cybersecurity Framework requires a report of such incidents to its Banking Supervision Director. While it is understood that cyber incident reporting requires different structures for different purposes, stages and sectors, it is also clear that the current institutional structure for reporting within the Nigerian financial sector is weak and inadequate. The cyber incident reporting function appears lost in a web of complex institutional arrangements.

When compared against cyber incident reporting initiatives and guidelines issued by regulators in the UK and US, it becomes evident that Nigeria needs a clear structure for cyber incident reporting framework which encompasses all cyber-related issues and is constantly reviewed to ensure effective control and management of cyber vulnerabilities.

Uneven Supervision and Enforcement

The factor of uneven supervision and enforcement is closely tied to the issue of inadequate regulatory frameworks. At the 2017 annual meeting of the NeFF's Steering Committee, titled "Operationalising a Four-Sided Approach to Preventing Fraud", it was noted that Law Enforcement was one of the four major issues affecting the banking sector.[166] Regulators need to actively and effectively conduct regular supervision of FIs to identify existing and evolving security risks (some of which may have no provisions under the law), and enforce corrective actions.

Without supervision, financial regulators are unable to understand the scope and depth of the cyber threat landscape and this itself is a governance gap in the supervisory framework. Effective supervision requires the enforcement of regulation in FIs. Besides, fines are

[166] NeFF, 'A Changing Payments Ecosystem: The Security Challenge - Annual Report 2016' 15.

sometimes insufficient to enforce compliance by FIs' and regulators need to develop the expertise which allows them to supervise FIs when carrying out relevant remedial programmes for cybersecurity deficiencies.

Meanwhile, Courts have expressed concerns for the abuse of the legal process in instances where the complainant files a petition for the same offences at two different institutions[167] noting that this may lead to a duplication of complaints and consequently fragment the effectiveness of the judicial process or pose fine/sentencing challenges for the defendant where they are investigated and prosecuted by various agencies on an identical charge.[168] On the other hand, the safe harbour provided for top public officials in Section 308(1) of Nigeria's 1999 Constitution presents a challenge. This provision contains an immunity clause which renders the prosecution of government officials still in office almost impossible, and thus allows for the cybercrimes aided by, facilitated by or committed through FIs to be done with impunity.[169] Although, this challenge may be countered if proceedings are brought under civil law as stated under section 308(2).

In the same vein, uneven enforcement is reflected in the conduct of the EFCC, who has been shown to take prompt actions towards cybercrimes committed by certain individuals, but not towards FIs and top public officials. According to the Nigerian Inter-Bank Settlement System, challenges to the EFCC's investigation process and apprehension rate include the lack of well-defined laws and lack of cooperation between law enforcement agencies and FIs.[170]

Political Interference

Section 11(2)(f) of the CBN Act 2007 states that "a person shall not remain a Governor, Deputy Governor or Director of the Bank if he is removed by the President: provided that the

[167] Diamond Bank Plc v H.R.H. Eze (Dr) Peter Opara & Ors (2018) 7 NWLR (Pt 1617) 92 and EFCC v Diamond Bank Plc and Ors (2018) 8 NWLR (Pt 1620) 61.
[168] Onyema and others, 'The Economic and Financial Crimes Commission and the politics of (in) effective implementation of Nigeria's anti-corruption policy' 23.
[169] Obuah, 'Combating corruption in a "failed" state: the Nigerian Economic and Financial Crimes Commission (EFCC)' 45.
[170] Nigerian Inter-Bank Settlement System, '2014 E-payment Fraud Landscape in Nigeria' 10 <http://www.nibss-plc.com.ng/wp-content/uploads/2015/03/Fraud-Landscape-2014.pdf> accessed 31 March 2019.

removal is supported by two-thirds majority of the Senate". The intention of this provision was to pursue the fulfilment of the CBNs mandate to maintain independence in the discharge of its functions, by subjecting the appointment and removal of board members to Senate approval.[171]

For appointments under the Act however, there seem to be a patronage culture which may be another factor responsible for allowing the CBN to operate under government interference and control. Indeed, in 2014, the previous CBN Governor, Lamido Sanusi was sacked by the former President of Nigeria, Goodluck Jonathan, for expressing "serious concerns" on the failure of the Nigerian National Petroleum Commission to account for oil revenues amounting to $20bn.[172] The Ex-Governor notes the use of customers' funds by bankers in purchasing luxuries and investments, and confirms that their conduct was unregulated as the institution responsible for coordinating financial supervisors, the Financial Services Regulation Coordination Committee, had not set up a meeting in two years.[173] This exposes problems in the supervisory framework as well as governance and accountability issues relating on the form of checks and balances required to enhance efficiency. Without regular meetings between supervisors and FIs, systems are left unmonitored and security risks unchecked, which in turn leads to ineffective risk management.

The appointments by the current government[174] and those of the past government[175] reflect an unequal representation of the three ethnic groups as persons from the President's ethnic group usually make up the majority of board members, contrary to Section 14(3) of the 1999 Constitution (Amended) on Federal Character Principles. The framework in place for ensuring the CBNs independence is weak. While the President should ideally be answerable to the Senate regarding certain issues, this is often not the case as 'the ruling party controls the

[171] CBN, 'A Brief of the Central Bank of Nigeria Act 2007' <https://webcache.googleusercontent.com/search?q=cache:4a0pOBKsHbEJ:https://www.cbn.gov.ng/OUT/PUBLICATIONS/PRESSRELEASE/GOV/2007/PR3-7-07.PDF+&cd=4&hl=en&ct=clnk&gl=uk> accessed 5 March 2019.
[172] S. Chayes, *Thieves of State: Why Corruption Threatens Global Security* (W. W. Norton 2015) 130.
[173] G. Serkin, *Frontier: Exploring the Top Ten Emerging Markets of Tomorrow* (Wiley 2015) 179.
[174] CBN, 'The Board' <https://www.cbn.gov.ng/AboutCBN/TheList.asp> accessed 5 March 2019.
[175] M. Mawere and S. Awuah-Nyamekye, *Harnessing Cultural Capital for Sustainability: A Pan Africanist Perspective* (Langaa RPCIG 2015) 40.

Senate'[176]. Indeed, Nelson confirms that appointment to public service rarely involves consideration of administrative capabilities, but rather loyalty, reputation, political, ethnic and social affiliations.[177]

Similar to Nigeria, the Chair of the FRS in the US is appointed by the President and then confirmed by the Senate. However, removal of the FRS Chair by the US President can only be done "for cause"[178] such as negligence in the discharge of functions, incompetence or misconduct,[179] but cannot be "for no reason or a bad reason".[180] Meanwhile in the UK, the Governor of the BoE is appointed by the Chancellor of the Exchequer with the consent of the Prime Minister and the Monarch. Taking a different approach, removal of the BoE Governor may only be done by the Bank with the approval of the Chancellor for non-attendance at meetings of the court for at least 3 months without permission, bankruptcy or the inability or incompetence to carry out functions of the role.[181]

Although removal of the heads of the central banks in the UK and US requires some government involvement, it can be seen through the structures that it is not based solely on the influence or directions from the government. Evidently, the Nigerian structure is formed in a way which allows the government exercise dominant influence on the institution, such that the CBNs President may be removed regardless of the cause. Beyond this, a similar institutional challenge exists with the EFCC, whose Chair is appointed by the President and may be removed by him for reasons including satisfaction by the President that it is not in the interest of the agency or the public.[182] Government involvement in setting governance frameworks that inform reflexivity has been argued to have vested interests in limited

[176] S. Adejumobi, *Governance and Politics in Post-Military Nigeria: Changes and Challenges* (Palgrave Macmillan US 2010) 96.
[177] M. Nelson, *Guide to the Presidency* (Taylor & Francis 2015) 1158.
[178] 12 U.S. Code § 242.
[179] Robert Eisenbeis, 'Can the President Fire the Chairman of the Federal Reserve?' (*Cumberland Advisors,* 10 January 2019) <https://www.cumber.com/can-the-president-fire-the-chairman-of-the-federal-reserve/> accessed 8 February 2021.
[180] Peter Conti-Brown, 'The Institution of Federal Reserve Independence' (2015) 32 Yale Journal on Regulation 257, 294.
[181] The Bank of England Act 1998, the Charters of the Bank and related documents, Section 8(1).
[182] EFCC Act 2004, Section 3(2).

reflexivity, retaining oligarchy, political benefits and social connections.[183] A question thus arise as to how the interest of the agency, or the interest of the public is to be ascertained.

Challenges to reflexivity in Nigerian FIs cybersecurity regulation go beyond gaps in legislation and exposes deficiencies inherent in its governance structures, to the extent, therefore, that these structures continue to pose threats to the effective and sustainable implementation of regulatory frameworks. Sustainability, as an essential premise of reflexive governance, is very critical due to the evolving and recursive challenges of modernity.[184] In order to achieve reflexive structural adjustments without any opposition from political influences, 'intentional and sustained attempts' must be made by engaging communications amongst various stakeholders, informing reflection about regulatory and societal environments for the purpose of modifying initiatives and re-evaluating practices,[185] and coordinating adoption and implementation of frameworks. In short, it is argued that measures directed at fixing existing governance structures is a key starting point for addressing issues in its cybersecurity regulation.

6.8 Conclusion

Nigeria has a promising approach to regulating cybersecurity risks. With thorough implementation, its approach could mitigate the cyber risks associated with the growing adoption of technologies, whilst still promoting financial innovation. The approach, while closely similar to the US approach is not as the generally relaxed approach of the UK. Although, we can see that the UK and US does a fairly better job with sanctioning and enforcement.

It is recommended that Nigeria learns from what has worked in both countries approach to enforcement. First, it is advised that Nigeria adopts an NIS Regulation to provide for a sector-wide data and IT security regulation. This could be done by adapting the UK NIS

[183] Feindt and Weiland, 'Reflexive governance: exploring the concept and assessing its critical potential for sustainable development. Introduction to the special issue' 670.
[184] James Meadowcroft and Reinhard Steurer, 'Assessment practices in the policy and politics cycles: a contribution to reflexive governance for sustainable development?' (2018) 20 Journal of environmental policy & planning 734, 739.
[185] Feindt and Weiland, 'Reflexive governance: exploring the concept and assessing its critical potential for sustainable development. Introduction to the special issue' 668 - 669.

Regulations 2018, taking into account the differences and similarities of the threat landscape and the economic capabilities. The implementation of such law, however, may be in form of introducing correct enforcement practices, creating new enforcement authorities and/or amending the remit of existing ones and removing duplicate agencies.

Second, it is essential to improve the capabilities of relevant personnel through training and threat testing/exercises. This will ensure staff are up to date in identifying, monitoring and mitigating cyber threats and attacks. In doing so, regulators and law enforcement agencies in Nigeria must toughen up measures in dealing with FIs by imposing compliance with higher governance standards on relevant issues e.g. reporting requirements, internal and external control processes etc. This recommendation is based on the notion that operational risk management relies on effective internal/external processes as well as timely disclosures.[186]

Third, threat reporting in the financial sector to regulators must be improved. It is recommended structures enhancing the monitoring and collation/reporting of cyber incidents be harmonised and effectively implemented across FIs and that regulators firmly exercise their legal mandates in order to enforce data quality and accuracy of incidents reported. Harmonisation of banking policies and procedures will also help prevent fragmented reporting of cyber risks[187]. Meanwhile, a review of gaps in existing legislation will help oversee an overall improvement in cybersecurity practices, in the hope that it will also revamp critical governance issues inhibiting enforcement efforts. As Van Brunschot et al note, law enforcement has the tendency to significantly enhance risk management.[188]

Further, there needs to be improved disclosure of data on banking practices i.e. making up-to-date quantitative and qualitative data on financial cybercrimes readily accessible and available through its quarterly or annual reports to promote transparency and facilitate policy recommendations. The availability and accessibility of such data may then be used in carrying out a detailed assessment of IT assets, networks and systems. In this regard, the CBN is advised to learn from the FCA and FFIEC and publish reports on its supervisory

[186] W. Bank, *World Bank Annual Report 2004* (World Bank 2004) 30.
[187] T. Tropina and C. Callanan, *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security* (Springer International Publishing 2015) 36.
[188] E.G. Van Brunschot and L.W. Kennedy, *Risk Balance and Security* (SAGE Publications 2007) ix.

practices which reflect many aspects of current best practice amongst the institutions it regulates. This should also include the provision for a centralised government organisation to be responsible for the collation and publishing of reports on cybercrime statistics.[189]

Lastly, there needs to be clarity regarding institutional structures, over who is responsible for what aspect of cybersecurity at a particular level as well as clear boundaries i.e., a properly defined institutional structure and framework for coordination and function among institutions. This is to address the issue of overlaps and gaps in the various roles of financial regulators which have in the past led to oversight and conflicting approaches.

[189] Olayemi, 'A socio-technological analysis of cybercrime and cyber security in Nigeria' 122.

Chapter 7. Lessons Learned and Future Implications

The aim of this thesis was to contribute to further learning on the cybersecurity regulatory frameworks in the UK, US and Nigerian financial services sector. The research conducted within this thesis was extensive, involving wide considerations of risk management theories in the assessment of regulatory frameworks, and specific reflexivity practices in the case studies. Still, this thesis represents only a part of the many angles to the challenges of cybersecurity risk management in the financial services sector, robustly exploring and comparing the effectiveness of self-regulatory and criminal justice responses in mitigating cybersecurity risks in the financial sector.

The importance of the findings of this thesis are considered under the lens of the major theme, reflexivity, with the expectation that it would inspire learning in FIs, regulators and government organisations. Among the solutions explored was the maximisation of reflexivity's potential in the face of changing risks, values, institutions, regulations, jurisdictions. The thesis contributes to debates regarding the role of reflexivity in regulation and risk management and endeavours to steer policies of accountability, adaptability, inclusivity, enforceability, interactivity and proactivity. The thesis found that while reflexivity appears to increase the potential for effectiveness in regulation, it may not always produce better regulation as for instance, adapting the regulatory frameworks of the US in Nigeria did not exactly lead to effective regulation of cybersecurity risks. Accordingly, the research sought to explain why this was the case and observed that reflexive learning may be compromised due to factors such as inadequate training, insufficient funding and resources, political interference, weak disciplinary systems and structural chaos.

Self-regulatory responses are significant for dealing with the risks of cyber threat and attacks by influencing conduct, requiring implementation of best security standards and, criminal justice responses are characterised by external intervention for attributing liability and enforcing compliance for security breaches. On the other hand, if not well implemented, either of both approaches may not be effective in mitigating cybersecurity risks. Traditional forms of regulation, as can be observed, are altogether ineffective and inadequately suited in addressing evolving cybersecurity risks which are by nature largely uncertain.

Based on this, we considered alternative models to law and regulation in literature exploring new forms of governance, reflexive modernisation and risk regulation. Despite the many discussions around reforming regulatory approaches, the governance and regulation of cybersecurity risks in the financial sector call for greater consideration.

Hence, this chapter highlights the practical and theoretical lessons learned from the preceding chapters that could be drawn for more effective and reflexive governance, briefly defining the research limitations; implications for academia, financial institutions, regulators and policymakers; outlining the key findings relating to the research questions; drawing policy conclusions and offering recommendations. Given the findings of the current research, this chapter will conclude with an explanation of next research steps to advance this area of inquiry.

7.1 Key Findings and Observations

By considering the question of how self-regulatory responses co-exist with criminal justice responses to ensure effective regulation of cybercriminal conduct and impose liability for cybercrimes in the financial services sector, this thesis was able to discuss and examine challenges to and drivers of an effective cybersecurity risk regulatory framework.

In solving the *main research question,* ancillary *sub-questions* which were discussed helped to facilitate the structure and execution of the research objectives. The Research Questions were explored using secondary data analysis and a review of literature within the research area. These questions were primarily addressed through an evaluation of data on the prevalent cyber risks in each of the jurisdictions, sanctions imposed on financial institutions by regulators, cybersecurity risk management approaches implemented by financial institutions and legislation on cybersecurity. The thesis sought to provide answers to the research questions by exploring symbiosis of autopoietic systems and highlighted the need for the coexistence of criminal justice and self-regulatory systems in which the different actors participate in a networked regulatory environment towards the development of a regulatory system influenced by structures and repeated processes of actions, reactions, learning, communication and change discussed in the earlier chapters. Each chapter reflects these themes identifying how effective regulation may be achieved by regulators taking

advantage of the flow of natural interactions and participations among themselves and between the regulated, encouraging efficient communication between the participants and motivating them to facilitate regulatory processes, thereby allowing feedback to be received and enabling informed responses.[1]

Major findings for the main research question: a. *How do self-regulatory responses co-exist with criminal justice responses to ensure effective regulation of cybercrimes and impose liability for cybersecurity failures in the financial services sector?*, suggest that sanctions imposed on financial institutions may not necessarily achieve a deterrent effect, cybersecurity risk management approaches taken in the sector have not been fully reflexive and cybersecurity legislation which may enhance reflexive governance of cybersecurity risks have either been overlooked, partially implemented or inadequately enforced.

Also apparent was the difference in prevalent cyber risks in the UK and US financial institutions from those in Nigeria. Indeed, some of the differences in the cybersecurity challenges for the jurisdictions may be due to their levels of development and other factors. Nevertheless, Nigeria, having a similar legal custom with the UK and USA with regards to common law practices will facilitate this evaluation of how Nigeria may draw lessons from the UK and US cases. The findings in sub-question i. *How do jurisdictions identify the key cyber risks and design appropriate risk management systems, and what commonalities and divergences exist?*, reveal that threats in the UK and USA typically involve data breaches, phishing, ransomware and DDoS attacks, whereas in Nigeria these threats include scams which manifest in terms of online transfers and insider abuse. Although, there have been reports of phishing in Nigeria with, however, little evidence. As the threats experienced within these jurisdictions are different, the response regimes are also different. However, the question of their appropriateness involves many considerations as these cannot easily be drawn from practice.

The sections on self-regulatory fundamentals were vital in answering sub-question ii. *How effective are the self-regulatory responses in each jurisdiction for dealing with existing and emerging cyber risks in their FIs and how do they co-exist with criminal justice responses?* The effectiveness of the self-regulatory responses in dealing with cyber risks

[1] Murray, 'Symbiotic Regulation' 227 - 228.

varied across each jurisdiction. An overall examination of data on cyberattacks from the previous years in each jurisdiction indicate an increase in incidents and, thus, may suggest inadequacies in the self-regulatory responses. While this may be true, it is also possible that even where responses have been suitable, they have had unintended consequences due to the changing nature of the risks involved. Given that, in the UK, it may be observed that frameworks such as intelligence-centred security processes, if thoroughly implemented may proactively help to identify and prepare against these threats. Common trends in the US suggest that the use of machine learning and simulation exercises, if appropriately co-ordinated may help mitigate against these threats.

Unlike the UK, a major observation in the US was the difficulty in finding information in one single document and hence, having to analyse multiple documents to form a conclusion. In Nigeria, however, reports from banks include measures such as routine on-site and off-site testing and a 'three lines of defence model'. Certainly, the use of a more specific term or practical evidence may be beneficial in explaining the meaning of routine in respect of the frequency in which testing is carried out. On the other hand, the 'three lines of defence model' appears to offer a comprehensive framework in form of a first line detect, response and recover function, further safeguard in terms of monitoring and guidance and independent assurance of the effectiveness of the system and frameworks. If implemented with strong accountability, it may help ensure effective cyber risk management.

A discussion on reflexivity in regulation and supervision indicate comparatively less desired outcomes in the UK, USA and Nigeria in terms of cybersecurity objectives as challenges such as inadequate disclosures and a voluntary nature of regulatory guidelines appear to raise concern of gaps in the regulatory frameworks. Furthermore, the Nigerian case reveals a lack of systems of accountability, which helps us understand issues of transparency and governance in the financial institutions.

The accountability quagmire in Nigeria is further buttressed by findings in sub-question iii. *How effective are criminal justice responses in imposing liability for cyber offences in the financial services sector, where self-regulation has failed?,* as it can be seen clearly that inadequate legislation, poor enforcement, insufficient funding and resources, political interference and lack of independence of regulators and authorities involved in

supervision and enforcement were noted as main causes of ineffectiveness of the criminal justice responses. More so, majority of its legislation indicate a replication of US models without a replication of its practice. Unlike Nigeria, less political interference may be observed in the UK and the US financial services sector as appointment to public service is usually by skill and experience, than patronage. Evidence from the UK case, also suggests a deliberate omission by the government in implementing some relevant regulations in the sector, ultimately leaving it to police critical cyber risk management functions itself. As Beck observes, "[this] leaves the industries with the primary decision-making power but *without* responsibility for side effects, while politics is assigned the task of democratically legitimating decisions it has *not* taken and of 'cushioning' technology's side effects".[2] Meanwhile, a major concern in the US case is the myriad of data breach notification requirements across its States which produce legislative inconsistencies.

A view of legislation through the lens of reflexivity also indicate that self-reflection, stakeholder participation, flexible response capabilities and adaptive enforcement are effective means for enhancing cybersecurity legislation governing financial institutions.

7.2 Research and Theory Implications

The research adds new dimensions to the discussion on the reflexivity of risk, in particular, cybersecurity risks. Significant implications have been drawn from the findings in this thesis for scholars across varying disciplines due to the interdisciplinary nature of the research, financial institutions, policymakers, regulators and enforcement agencies in both developed and developing institutions.

This thesis is the first to comparatively explore reflexive approaches in the cybersecurity risk regulatory frameworks of financial institutions. Past studies have mostly focused on risk transfer approaches[3], resilience-based approaches for third party risks[4] and operational risk management[5]. More importantly, a recent study which explored the concept

[2] Beck and others, *Risk Society: Towards a New Modernity*, 213.
[3] Camillo, 'Cybersecurity: Risks and management of risks for global banks and financial institutions' 199.
[4] Haller and Wallen, *Managing third party risk in financial services organizations: a resilience-based approach*, 4.
[5] Abdullab Aloqab, Farouk Alobaidi and Bassam Raweh, 'Operational risk management in financial institutions: An overview' (2018) 8 *Business and economic research* 10, 20.

of reflexivity in relation to the financial sector, only explored the reflexivity theory in developing a strong quantitative finance model for profit-maximisation in international financial markets.[6] In addition, no extensive studies comparing developed and developing nations has been conducted.

Furthermore, the findings have also shown the lack or poor handling of investigation and prosecution by enforcement bodies with very little evidence of progress. In Nigeria, the corruption of the judicial and enforcement bodies has been found to hamper the effectiveness of criminal justice responses. Hence, knowledge capabilities, training and adequate funding are necessary to ensure the effectiveness of responses adopted.

7.3 Lessons and Policymaking Implications

This thesis has added to the growing pool of knowledge on risk theories as well as an understanding on regulatory developments within the financial sector. It also provides knowledge on theoretical perspectives on cybersecurity risk management concepts. Again, it offers important considerations for policy makers in evaluating existing cyber risk management regulatory frameworks and what changes can be made to enhance effectiveness.

In Chapter 3 of this thesis, we explored a wide range of literature including Beck's concept of reflexivity. The concept provided a solid theoretical foundation for analysis in the case studies. Although, as seen earlier, some ideas advanced by the concept had been criticised such as the equation of risks-to-risks perceptions[7]. Despite its shortcomings, this section draws upon the concept to provide some of the policy-related lessons learned from the case study jurisdictions. There are six policy-related lessons that arise from this research and these are discussed under the following headings: (a) funding; (b) cybersecurity legislation, guidelines and requirements; (c) information sharing; (d) incentivising regulation; (e) penalty and sentencing; and (f) annual reports, voluntary guidelines and policies.

---

[6] Yogesh Malhotra, *Beyond Model Risk Management to Model Risk Arbitrage for FinTech Era: How to Navigate 'Uncertainty'... When 'Models' Are 'Wrong'... And Knowledge'...'Imperfect'! Knight Reconsidered Again: Risk, Uncertainty, & Profit Beyond ZIRP & NIRP* (Princeton Quant Trading Conference, Princeton University 16 April 2016).

[7] Bergkamp, 'The concept of risk society as a model for risk regulation–its hidden and not so hidden ambitions, side effects, and risks' 1287.

Funding

Funding is one of the means of influence a government has to aid the implementation of its set objectives.[8] In the UK, the financial services sector is funded from the National Cyber Security Budget estimated at £1.9 billion in the National Cyber Security Strategy 2016 – 2021.[9] The US on the other hand, indicates its attention to enhancing cybersecurity of its assets and infrastructures by setting aside a yearly cyber security budget, with the one for year 2020 estimated at $17.4 billion dollars (an increase of $790million from the previous year).[10] By calculation the US yearly budget is about 15 times more than the UK five-year budget. In the Nigerian case, however, there are no comparable values as the last published cybersecurity strategy in 2014 makes no disclosure of the costs of budget.[11] Regardless, a major difference is the gap in funding between the UK and the US, which may also translate to a resource gap, depending on how the budget is executed, particularly with regards to the financial sector. However, it is important to note that a possible basis for the significant funding in the US is due to the different requirements of its many institutions.

While data on sector-specific budget is not available, it may be worth noting that inadequate funding is one of the challenges to the investigation and prosecution of cybercrimes adequately. Indeed, this has been observed in the Nigerian case, where lack of resource and funding hinders the effective implementation of legislation and encourages irresponsible and corrupt behaviour of relevant personnel. Also, lack of a recent evaluation on its cybersecurity policy and strategy reflect a poor reflexive approach as strategies of today quickly become risks for tomorrow due to their inadequacies, thus informing the need for new strategies.

[8] Beck and others, *Risk Society: Towards a New Modernity*, 219.
[9] HM Government, 'The UK Cyber Security Strategy - Protecting and promoting the UK in a digital world' 6 (November 2011) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> accessed 10 November 2020.
[10] White House, 'Cyber Security Funding' 306 <https://www.govinfo.gov/content/pkg/BUDGET-2020-PER/pdf/BUDGET-2020-PER-5-8.pdf> accessed 10 November 2020.
[11] Nigeria Computer Emergency Response Team, 'National Cyber Security Strategy' (December 2014) <https://www.cert.gov.ng/file/docs/NATIONAL_CYBESECURITY_STRATEGY.pdf> accessed 24 August 2018.

A major finding from the UK studies is its cherry-picking approach to cybersecurity legislation in the financial sector. For instance, its decision to implement the GDPR applicable to all sectors, including the financial sector and its selective implementation of the NIS Regulations, excluding the financial sector which is without a doubt an operator of essential services. It is unjustifiable that the financial sector was not specifically considered for a regulation that ensures the security of its network and information systems on the unclear basis that there are "provisions within [its] existing legislation which are, or will be, at least equivalent to those the NIS Directive specifies".[12] This appears not to have been carefully thought out as shortcomings relating to the exclusion of the financial sector, the voluntary compliance requirement and lack of prosecution of non-compliance were included in the concerns raised in the public consultation prior to the implementation of the NIS regulations.[13] Moreover, in response to the consultations, the government notes that a single incident could give rise to penalties under each of the regimes due to various offences and effects being considered.[14] Indeed, in cases where a financial institution's IT system failures and disruption result in the loss of personal sensitive data, the institution will no doubt face liability under both regimes.

The NIS Regulations provides an overarching legal framework on the security of network and information systems which if implemented appropriately will ensure the security of data and enhance privacy and thus, appears more relevant than the GDPR. In fact, 'security of network and information systems' in the Regulations refer to " the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems."[15] Unfortunately, the flexibility offered regarding implementation, giving member

[12] Department for Transport, Implementation of the NIS Directive DfT Guidance version 1.1 (December 2018) para 2.4 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/892104/implementation-of-the-nis-directive-dft-guidance-document.pdf> accessed 1 November 2020.
[13] Department for Digital, Culture, Media and Sport, Security of Network and Information Systems Public Consultation (August 2017) 7.
[14] Department for Digital, Culture, Media and Sport, 'Security of Network and Information Systems Government response to public consultation' (January 2018) 16.
[15] The Network and Information Systems Regulations 2018, Article 1(3)(g).

states options to decide their approach and sector applicability may be regarded as a disadvantage. The effects of this will in the long run be, socially and reflexively undesirable.

Compared to the UK DPA 2018 which offers specific provisions on requirements relating to 'security of processing',[16] 'designation of a data protection officer',[17] 'notification of a personal data breach to the Commissioner'[18] and 'penalties for breaches'.[19], a key finding for the US is the lack of consensus on a single or specific data protection and privacy legislation. The effect of this, being a patchwork of data breach notification requirement amongst States. Open to varied interpretations, outcomes such as legislative incoherence become the order of the day. The current regime in the US is heavily dependent on self-regulatory guidelines formed by its regulators from which financial institutions may draw upon as best practices. Although, the GLBA 1999 does make some provision for the privacy and protection of sensitive personal financial data.

The GLBA 1999 also contains a provision similar to the UK NIS Regulations requiring operators of essential services to "take *appropriate* and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems [and to prevent and minimise impact of security incidents] on which their essential service relies."[20] The GLBA 1999 provides that financial institutions "shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are *appropriate* to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."[21] One common ground in both provisions is the appropriateness of cybersecurity measures which may take the form of technical (including physical) and organisational (administrative) safeguards. Of relevance are the terms technical and organisational which imply that effective cybersecurity measures go beyond practical technological methods and require an integration of people, procedures and policies to ensure accountability in the process. As Beck argues, "legal and institutional

[16] Data Protection Act 2018, Section 107.
[17] Data Protection Act 2018, Section 69.
[18] Data Protection Act 2018, Section 67.
[19] Data Protection Act 2018, Section 157.
[20] The Network and Information Systems Regulations 2018, Article 10.
[21] 16 C.F.R. § 314.3(a).

conditions will be created to enable ongoing process of social learning and experimentation to continue against existing restrictions."[22] This argument appears to echo the idea of coexistence of criminal justice and regulatory responses to ensure effectiveness.

In contrast, the Nigerian regime recently adopted in form of the NDPR 2019, in form of what appears to be a lesson learned from the GDPR, shows no reflexive approach to implementation as relevant provisions such as the data breach notification requirement appear to have been side-lined. For a country still at growing levels of development with not yet advanced cybersecurity measures, one would expect that information relating to data breaches would facilitate self-learning processes towards reproduction of changes in its systems. As such, one take home lesson for Nigeria is that without an understanding of the problem, any responses offered would likely be ineffective or inappropriate. On the other hand, Nigeria currently has no NIS-type regulations. A possible provision in Section 19(3) of its Cybercrimes Act 2015 which could have been interpreted to accommodate such measures is a failed attempt at placing a duty on financial institutions to implement 'effective counter-fraud measures'. Fraud is not the only threat to security in financial institutions and the question as to what safeguards guarantee effectiveness also arises. Besides, as discussed in Chapter 6, the provision is flawed as it shows no regard for consumer protection.

The crux of this lesson is that while the UK has currently developed its legislation to effect a uniform approach to personal data security, it needs to extend the implementation of the NIS Regulations to the financial sector. As it stands, the US may benefit from a single data protection and privacy legislation. Although, given the broad provisions of the GLBA 1999 which also cover for detection, prevention, response and continuity,[23] it arguably may not require a UK-type regulation. In the same light, Nigeria, is clearly married to a pattern of legislation that discourages responsibility and transparency, may learn by adopting a streamlined UK-type NIS regulation and amendment of laws which hinder cybersecurity regulatory objectives.

[22] Beck and others, *Risk Society: Towards a New Modernity* 235.
[23] 16 C.F.R. § 314.4 (b)(3).

Information Sharing

Another major lesson to learn from Beck is the idea that "[Collaboration] . . . involves consultation, interaction, negotiation, network: in short, it is perceived as the interdependency and process character in the context of the responsible, affected and interested agencies and actors from the formulation of programmes through the choice of measures to the forms of their enforcement."[24]

In the UK, there are a few regulatory guidelines relating to the sharing of information on 'material' cybersecurity breaches to the FCA.[25] In the absence of what amounts to 'material' breaches¸ its interpretation therefore relies on a subjective test. By contrast, the US has many guidelines regarding the communication of cybersecurity risks and data breaches amongst financial institutions. However, there is no clear structure on the processes or the extent to which this information may be communicated.[26] In particular, it is noted that due to the multitude of regulators involved in the process, different actions are taken, resulting in the undermining or enhancement of information sharing.

Compared to the UK and US, in Nigeria, there is only one guideline relating to the sharing of information on cybersecurity incidents by financial institutions with regulators. This requires the submission of a report on the outcome of self-assessment cybersecurity exercises to the Banking Supervision Director of the CBN.[27] Meanwhile, tools to assist in the cybersecurity self-assessment have been identified as those adopted by the USA. The problem with this is that the Nigerian financial sector does not appear to have properly adapted these tools for use. There is no learning from copy and paste, without an analysis or understanding of the idea behind what has been copied. Besides, "enabling self-criticism in all its forms is not some sort of danger, but probably the only way that mistakes that would sooner or later destroy our world can be detected in advance."[28] The US CAT comprises of a two-part test which includes the threat intelligence and collaboration, a domain which assesses and

[24] Beck and others, *Risk Society: Towards a New Modernity*, 199.
[25] Principle 11 and Sup 15.3 FCA Handbook, Financial Conduct Authority, 'Good cyber security – the foundations' (2017).
[26] V Gerard Comizio, Behnam Dayanim and Laura Bain, 'Cybersecurity as a global concern in need of global solutions: an overview of financial regulatory developments in 2015' (2016) 17 Journal of Investment Compliance 101, 102.
[27] CBN, 'Risk-Based Cybersecurity Framework and Guidelines for DMBs and PSPs' (October 2018) para 4.3.
[28] Beck and others, *Risk Society: Towards a New Modernity*, 234.

monitors threat intelligence and information sharing. The Nigerian guideline mentions cyber-threat intelligence which if analysed appropriately may promote proactive cybersecurity strategies, but was silent on collaboration, even though it requires a report of these threats to the Banking Supervision Director of the CBN[29]. Thus, raising questions as to whether this is merely a problem with implementation or a transparency issue.

A tool similar to the US CAT adopted in the UK, is the CBEST which aims to enhance learning and awareness of the cyber threats capable of threatening the stability of the UK financial system. Both the CAT and CBEST are useful tools to assist financial institutions in the assessment of the effectiveness of their cybersecurity risk management frameworks. By reviewing and readapting its current frameworks, Nigeria can enhance its approach to assessing cybersecurity resilience in its financial institutions.

Incentivising Regulation

Another key observation from the UK studies is the wedding of regulations to incentives i.e. the carrot-and-stick approach to learning where evidently compliant financial institutions receive rewards in form of discount on fines imposed, while non-compliant institutions are bound to face the full extent of the law. This approach in many ways underscores the principle of reflexivity as it fosters self-regulation in form of risk management best practices by financial institutions (carrot) which if ineffective, results in a threat of or actual external regulatory intervention to enforce compliance. A similar approach is observed in the US where the CFPB consider measures such as cooperation, previous regulatory proceedings, degree and scope of the breach and the proportionality of the institution's cybersecurity procedures with its size in order to initiate enforcement. In contrast, the UK's FCA focuses on disgorgement, discipline and deterrence as identified in Chapter 4.

A key difference between both approaches is that compared to the UK where aggravating factors may include advantage gained, the US recognises previous regulatory proceedings arguably involving considerations of repeated misconducts which may result in escalating sanctions to deter misconduct. Meanwhile, like the US, the UK also regards the cooperation of financial institutions as a major deciding factor as can be seen in the *Tesco*

[29] CBN, 'Risk-Based Cybersecurity Framework and Guidelines for DMBs and PSPs' para 6.1.5.

case where fines were discounted due to cooperation with investigation and remedial actions. In the Nigerian case, however, such conclusions cannot be drawn due to the limited information available.

Penalty and Sentencing

The penalty and sentencing approaches to cybersecurity in the UK, US and Nigeria are different. More so, because of their different regulatory regimes and the nature of the offences. Also, in the UK and US, there are no direct provisions for criminalising cybersecurity breaches in financial institutions.

Under UK legislation, financial institutions may face high fines of up to £17 million under the NIS Regulations and up to €20million or 4% of their annual turnover under the DPA 2018. In the US, there are no single set fines for cybersecurity breaches. Generally, US regulators have been observed to impose varying fines ranging from $420,000 in the Citibank case to $575 million in the *Equifax* case. However, in some of its States, data violations may attract up to $7,500 for each intentional violation[30] and in others specific to financial institutions may include revocation of license and fines of up to $2500 dollars per day.[31] One major problem with fines on intentional violation is the obvious requirement of intent, which may not easily be proven in the case at hand. Similar revocation powers are also vested in the UK's FCA in accordance with carrying out its objective of 'protecting and strengthening the integrity of the financial system' under the FSMA 2000[32], and may possibly be extended to conducts which compromise the integrity of data in the financial system. In Nigeria, fines of up to N10 million (£16,666) may be imposed under the NDPR 2019.i.e. over 1,000 times less than the UK provisions. Under the Cybercrimes Act 2015, there is also a criminalisation of identity theft involving staff of financial institutions attracting a fine of up to N5 million (£8,333), or 7 years imprisonment or both.[33]

There are some observations of the UK and US reluctance to pursue criminal charges in cases of cybersecurity breaches in its financial institutions possibly due to concerns

[30] California Consumer Privacy Act 2018, Section 1798.155(b).
[31] 23 NYCRR 500, Section 44(1)(b).
[32] As amended by the Financial Services Act 2012, Section 206.
[33] Cybercrimes Act 2015, Section 22(1).

over discouraging innovation and the difficulty in establishing collective accountability as discussed in Chapter 3 and overregulation which leads to counterproductive sentencing. While these concerns are valid, financial institutions may benefit from a model which imposes sanctions on those involved in setting broad security strategies in an organisation such as the Chief Information Security Officers. The proposed model may be called a Strategic Accountability Model (SAM) based on the notion that institutions are made up of individuals who can be liable for 'failing in their duty to implement reasonable cybersecurity safeguards or to exercise due diligence, through action or inaction'.[34] In such a case, the CIO of Equifax would have been criminally liable for recklessness as to the implementation of strategies which he ought to have supervised as part of his duty of care to the institution and its customers, but described as a "lower-level responsibility that was six levels down" below him[35] i.e. liability imposed for breaching the duty of care owed to the institution. The SAM does not seek to undermine but complement the system of collective responsibility for cybersecurity failures. Although, an extended discussion of the model is beyond the scope of this thesis and there is need for studies that look at the implications of individual and collective responsibilities for cybersecurity breaches. If successful, the model may enable a more accountable approach to cybersecurity operational decision-making processes. At the same time, an alternative approach to individual criminal liability might be the suspension of professional license of relevant individuals and a request for additional remedial actions like training before license is reissued. Such measures may promote reflexive learning and self-adjustments.

An additional lesson which can be learnt in penalty and sentencing is the four-tiered structure of the NIS fine regime, which relies on the material significance of the breach comprising of fines for non-compliance which do not give rise to a cybersecurity incident; fines for material non-compliance which has given rise to or has the likelihood of giving rise to a cybersecurity incident causing a service reduction; fines for material non-compliance which has given rise to or has the likelihood of giving rise to a cybersecurity incident causing a service disruption for a significant period of time; and fines for material non-compliance which has given rise to or has the likelihood of giving rise to a cybersecurity incident causing

[34] Fisse, 'The attribution of criminal liability to corporations: A statutory model' 279.
[35] US Senate, 'Equifax Report' 37.

a direct threat to life or substantially adverse effect on the UK's economy.[36] This Regulation reflects the concept of risk identification and prioritisation identified in Chapter 3 and provides competent authorities with guidance in issuing appropriate fines. Nigeria and the US could usefully learn from this approach, where more effective and proportionate fines could be issued and where state legislation providing inadequate and unclear fine regimes may be reviewed, respectively. Nigeria with its existing laws may benefit from a thorough implementation process to guarantee effectiveness of its penalty and sentencing provisions.

On the whole, this finding concludes that while the extensive fines imposed by financial authorities in regulating cybersecurity breaches are applauded, investigation and prosecution, are also measures which it may adopt to further improve effectiveness of the criminal justice responses to cybersecurity breaches. Where regulators have limited prosecutorial powers as in the case of the UK's FCA and US SEC, or are unable to initiate a proceeding for one reason or the other, it could refer cases to relevant authorities like the NCA and DoJ, respectively.[37]

Annual Reports, Voluntary Guidelines and Policies

Statements in annual reports of financial institutions examined in the case studies have suggested that majority of the measures adopted in most of the institutions are based on individual risk perceptions. While no country mandates inclusion of statements on cyber risk management, it is worth noting that the US SEC does provide guidance that these should be disclosed if they pose a risk to investors[38]. In addition, financial institutions in all three jurisdictions provide guidelines and policies, covering board and staff training, implementation of best security standards and cyber threat scenario exercises.

In summary, the findings discussed above show:

[36] NIS Regulations 2018, Regulation 18(5). ICO, 'Enforcement' <https://ico.org.uk/for-organisations/the-guide-to-nis/enforcement/> accessed 10 July 2021.
[37] By contrast, in Nigeria, the EFCC as one of the central regulatory and enforcement authorities is vested with powers to initiate prosecution.
[38] SEC, 'Commission Statement and Guidance on Public Company Cybersecurity Disclosures' (26 February 2018) 17 <https://www.sec.gov/rules/interp/2018/33-10459.pdf> accessed 10 November 2020.

1. There are a few differences in the cybersecurity risks experienced in developed and developing economies and the risk management frameworks adopted for mitigating cybersecurity risks, varies by country. In fact, frameworks adopted in developed countries appear to have many disparities.

2. Aspects of the regulatory regimes in the developed countries which may be ideal or applicable in developing countries, have been poorly implemented.

3. To improve effectiveness of the self-regulatory responses, factors to be taken into account in developing regulatory frameworks include funding, incentives, information sharing and participation.

4. An institution which reports cyber breaches and incidents does so with the aim of effecting a change, like a sinner who confesses their sins with a view to hope for the chance and beauty of a life of ease.[39] Hence, where financial institutions report cyber incidents, it must go all the way to reevaluate its cybersecurity systems and processes to redefine its direction towards preventing and mitigating against future threats.

5. Problems of information sharing and cyber incident reporting between law enforcement and financial institutions, and amongst financial institutions may be addressed restructuring relevant institutional frameworks and ensuring clarity and transparency of cyber incident communication requirements.

6. To improve effectiveness of criminal justice responses, the reshaping of inadequate legislation, activating of dormant regulations and implementation of criminal sanctions becomes extremely important.

It is hoped that the findings of this study will provide insights for legislation, boards of financial institutions, regulatory and law enforcement authorities, policy makers, and banks and their staff in developing and implementing cybersecurity best practices to mitigate against attacks and risks to their data, network and systems.

[39] Beck, *World Risk Society*, 138.

Summary of Recommendations

Regulators within the sector will need to intensify their efforts towards implementing necessary measures. In areas where there are conflicting mandates and low collaboration, clarity must be given on roles and division of labour, and intelligence sharing must be improved between the different regulators, to promote learning and inform actions. In the same vein, operational independence from corrupt political interference, appropriate funding, and training resources, are also part of the criteria for its effectiveness.

The creation of cybersecurity awareness by financial institutions will help ensure that customers understand basic steps to take in preventing cyber risks. In addition, institutions must put in place adequate and up-to-date cybersecurity training for all of its staff as even entry level staff may unknowingly pose a threat to cybersecurity procedures, where their system has been compromised. Indeed, "agents who must perform institutionalised actions must . . . be systematically acquainted with institutionalised meaning."[40] Financial institutions must also improve their behaviors towards adapting and implementing legislation, tracking, and publishing more data on cyber threat landscape, cyber breach incident breach reporting and invest in avenues which promote partnership with regulators and law enforcement authorities. Further research should also be conducted on the SAM to determine its viability and study the influence of allocating individual responsibility for cybersecurity breaches on the criminal justice objectives of retribution and deterrence.

In summary, countries must find ways to ensure the harmonised coexistence of their regulatory systems, and provide a well-structured ecosystem for coordinated cyber risk management and ultimately resilience enhancement. In light of this, the financial sector must first evaluate its institutional design and make necessary rearrangements. In particular, the Nigerian financial sector must pay attention to reflection and adaptation whereby the country is to be informed by its past security incidents and current threat landscape, which will serve as an instrument for its change and choice as to what laws to adopt or adapt.

[40] ibid 98 - 99.

7.4 Limitations of the Study

This research has conducted a detailed evaluation of the management and regulation of cybersecurity risks in the UK, USA and Nigerian financial sector. However, it is important to discuss some shortcomings observed during the research process.

First, conclusions reached in the cases studies may not be generalised beyond the specified target population. They create an understanding of the UK, USA and Nigerian financial services sector, and may only be adapted as findings and lessons learned for future research. As noted in the previous chapters, there were complexities in secondary data collation, which resulted in the exemption of relevant and comparative data, and the reliance on literature to explain causes. Hence, the extent to which findings may be applicable may be hampered by the inadequacy of data to provide a full picture of the current landscape.

Also, the FIs considered in the case studies were of limited sample size and do not represent all FIs in each of the jurisdictions. Although, the FIs examined together, however, aid analysis of risk management processes and lead to highly likely inferences. Indeed, to achieve a close reflection of the sector, information was drawn from leading banks in each jurisdiction. Factors considered in the selection of banks include their year of establishments, total assets, customer base and technological advancement. In particular, selecting banks based on their year of establishment may allow for a reflexive understanding of changing risks and risk management approaches over the years.

A number of primary data collection techniques such as surveys and interviews which have not been explored in this research due to lack of feasibility are substituted with financial and regulatory reports which discuss the relevant risks and security measures relevant to this research. In view of this, the law, theories and data examined in this thesis offer a meaningful basis for a critique of the cyber risk management and regulatory frameworks in financial institutions of the case studies and other global financial institutions.

In summary, the observations communicated in this research may well be seen as a reasonable representation of common attitudes of financial institutions in the case study countries to influence cybersecurity risk management processes and regulation.

7.5 How Can We Improve the Narrative?

Expanding the wealth, availability and accessibility of secondary datasets on cyber incidents in financial institutions will aid future research in addressing future cyber risk management and regulatory challenges. Importantly, such data will not only help develop the knowledge pool, but will help in closing gaps identified in this research. Collaboration with financial institutions, regulators and policymakers will also be beneficial in gaining first-hand insight into the sector. However, as this raises ethical concerns such as confidentiality, necessary arrangements and discussions should be initiated at the early stages of the research.

Using risk-specific data obtained from financial institutions on cyber incidents, future research may be able to test the correlation between risk levels and implemented responses. This data should also contain information on self-regulatory and criminal justice responses. Such analysis will assist relevant stakeholders in making informed decisions on policy implementation; cybersecurity risk management strategies; national and international responses; to make data readily available for future research and risk assessment; and to enhance accountability, credibility and reflexivity in regulatory processes.

Finally, additional studies may be conducted to explore the punishment appropriate for the SAM, especially taking into account the differences between sanctions as representations of moral judgements that deepen peoples law abiding moral beliefs and sanctions as exemplary processes that foster compliance with the law out of fear of consequences.[41]

7.6 In the End

The principal findings presented in this chapter, provide an insight to the successes of and challenges to the coexistence of criminal justice and self-regulatory responses in ensuring effectiveness in cybersecurity risk management. From the results presented in this chapter, it appears that collaboration is an important aspect of cybersecurity risk regulation in the financial sector that needs to be carefully developed.

[41] Kramer, *The ethics of capital punishment: A philosophical investigation of evil and its consequences*, 159.

While this research focuses on the analysis of structures and processes of law and institutions in testing effectiveness of frameworks, it is important to note that the true results of its effectiveness may also be drawn from data detailing successful cybersecurity risk prevention and mitigation in the sector.

Taking into consideration the nature of the risks being examined, findings indicate a major implication for implementing reactive approaches to regulation. Characterised by its failure to challenge existing norms, nature of systems, structures and policies,[42] today's reactive approaches that were at some point yesterday's proactive ones, are different from the proactive approach which involves continuous and systematic planning and implementation of early cybersecurity measures to prevent future risks. "Thus, there are fundamentally *two options* confronting each other in dealing with [cybersecurity] risks: removing the causes or [fighting against] the consequences and symptoms, which tend to expand markets".[43]

In the end, it would be a fallacy to think that self-regulatory responses can replace criminal justice responses or vice-versa; indeed, the success of both cybersecurity risk management lies in their coexistence. Cybersecurity risks will continue to evolve, but what the financial sector can and must do is to establish new institutional measures, including co-ordinating arrangements between key stakeholders, aimed at effectively managing existing risks and preparing for future risks. The effectiveness of both approaches is not built on the idea that the frameworks would achieve the results desired all of the time, but much more that through re-learning and re-adjusting processes, it would at the very least have measures in place to adequately respond to the impacts of successful cyberattacks and minimise the risk of future ones.

[42] Andrew Gouldson and Joseph Murphy, *Regulatory realities: The implementation and impact of industrial environmental regulation* (Routledge 2013) 8.
[43] Beck and others, *Risk Society: Towards a New Modernity* 175.

Summarising Chapter

This thesis explored reflexivity as a means to inform adaptive, resilient and effective cybersecurity risk management practices. It explored how Beck, in his works, defines and interprets the concept of modernised risks which provides context for the definition of cybersecurity risks adopted within this research and explicates the theoretical and research dimensions that underlie the concept of reflexivity, furthering the argument that the efficacy of self-regulation may only be fully reached with the intervention of the law. It also elaborates the work of Black, illuminating discussions on decentred approaches to regulation and the self-referential characteristics of autopoietic systems facilitated by symbiosis , which Murray describes as a 'control model that affords all participants in the regulatory matrix an opportunity to shape the evolutionary development of their environment'.[44]

The development of arguments in this thesis is based on the understanding of indirect influence of the law embedded in the concept of self-regulation. Such indirect influence as Majone highlights is the use of regulatory agencies responsible for "fact-finding, rulemaking, and enforcement" and identifies this an opportunity for seemingly more effective, policy methods without eliminating regulation.

The thesis challenged conventional beliefs about the positive impacts of reflexivity in regulation by discussing cases where reflexivity was effective and one where it failed noting that, in the absence of suitable practices, frameworks and the institutions, reflexivity may not produce required results for regulation, and thus may not always be something to strive towards. To address this gap, this thesis introduces new dimensions to the concept of reflexivity arguing that better reflexivity focuses on the foundation (why), structure (what) and maintenance (how), and not merely on the structure. That is to enjoy the benefits of reflexivity, the systems in place should be instructive; setting out detailed guidelines to direct and influence operations, preventive; regularly monitoring and supervising operations to ensure continuous resilience, and corrective; intervening in the event of an IT system failing where due diligence practices have been followed or not and imposing fines and/or sentences.

[44] Murray, 'Symbiotic Regulation' 224.

It has been argued throughout this work that to maximise the effectiveness of cybersecurity regulation, self-regulatory responses have to be carefully married with criminal justice responses. Particularly, incorporating the ways in which reflexivity has been theorised by proposing a regulatory framework involving participation, communication, collaboration and information sharing between all key actors and the repeated processes of change and learning that characterise 'the state in which modernisation 'becomes its own theme'' i.e. exercising constant self-reflection aimed at continuous self-development.

Bibliography

Books, Journal Articles and Publications

Achterbergh J and Vriens D, *Organizations: Social Systems Conducting Experiments* (Springer Berlin Heidelberg 2010)

Achua JK, 'Corporate social responsibility in Nigerian banking system' (2008) 3 Society and Business Review 57

Adam B, Beck U and Van Loon J, *The Risk Society and Beyond: Critical Issues for Social Theory* (SAGE Publications 2000)

Adejumobi S, *Governance and Politics in Post-Military Nigeria: Changes and Challenges* (Palgrave Macmillan US 2010)

Adekoya AA, 'Corporate Governance Reforms in Nigeria: Challenges and Suggested Solutions' (2011) 6 Journal of Business Systems, Governance and Ethics 38

Aguilar LA, *Boards of directors, corporate governance and cyber-risks: Sharpening the focus* (2014)

Ajibo KI, 'Risk-based regulation: The future of Nigerian banking industry' (2015) 57 International Journal of Law and Management 201

Akinyomi OJ, 'Examination of fraud in the Nigerian banking sector and its prevention' (2012) 3 Asian Journal of Management Research 182

Aliyu AA and Tasmin R, *Information and Communication Technology in Nigerian Banks: Analysis of Services and Consumer Reactions* (2012)

Almansi AA, 'Financial sector's cybersecurity: regulations and supervision' (2018) The World Bank

Aloqab A, Alobaidi F and Raweh B, 'Operational risk management in financial institutions: An overview' (2018) 8 *Business and economic research* 10

Anderson R and others, 'Measuring the Changing Cost of Cybercrime' (2019) The 18th Annual Workshop on the Economics of Information Security (WEIS) 1

Arbel-Ganz O, 'Formal and Informal Regulatory Networks: Deliberative Policy Formation in Israel'

Ariff M, Farrar J and Khalid AM, *Regulatory Failure and the Global Financial Crisis: An Australian Perspective* (Edward Elgar Pub. 2012)

Awhefeada UV and Bernice OO, 'Appraising the Laws Governing the Control of Cybercrime in Nigeria' (2020) 8 Journal of Law and Criminal Justice 30

Baldwin R and Black J, 'Driving Priorities in Risk-based Regulation: What's the Problem?' (2016) 43 Journal of Law and Society 565

Baldwin R, Cave M and Lodge M, *Understanding Regulation: Theory, Strategy, and Practice* (OUP Oxford 2012)

Baldwin R, Scott C and Hood C, *A reader on regulation* (Oxford University Press 1998)

Ballou T, Allen JA and Francis K, 'US Energy Sector Cybersecurity: Hands-Off Approach or Effective Partnership?' (2016) 15 Journal of Information Warfare 44

Bank W, *World Bank Annual Report 2004* (World Bank 2004)

Barrett D, Weiss MM and Hausman K, *CompTIA Security+ SYO-401 Exam Cram: Comp Secu SY04 Auth ePub _4* (Pearson Education 2015)

Bassett WH, *Clay's handbook of environmental health* (Spon 1999)

Basu K and Cordella T, *Institutions, Governance and the Control of Corruption* (Springer 2018)

Beck T, Cull R and Jerome A, *Bank privatization and performance: Empirical evidence from Nigeria* (The World Bank 2005)

Beck U, *Ecological Politics in the Age of Risk Polity Press* (Cambridge 1995)

Beck U, *World Risk Society* (Wiley 1999)

Beck U, 'Critical theory of world risk society: a cosmopolitan vision' (2009) 16 Constellations 3

Beck U and others, *Risk Society: Towards a New Modernity* (SAGE Publications 1992)

Bergkamp L, 'The concept of risk society as a model for risk regulation–its hidden and not so hidden ambitions, side effects, and risks' (2017) 20 Journal of Risk Research 1275

Berleur JJ and Brunnstein K, *Ethics of computing: codes, spaces for discussion and law* (Springer Science & Business Media 1996)

Bidgoli H, *Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations* (Wiley 2006)

Black J, 'Decentring Regulation: Understanding the role of regulation and self-regulation in a'post-regulatory'world' (2001) 54 Current legal problems 103

Black J, 'Critical reflections on regulation' (2002) 27 Australian Journal of Legal Philosophy 1

Black J and Baldwin R, 'When risk-based regulation aims low: A strategic framework' (2012) 6 Regulation & Governance 131

Blind K, Petersen SS and Riillo CA, 'The impact of standards and regulation on innovation in uncertain markets' (2017) 46 Research Policy 249

Bonner L, 'Cyber risk: How the 2011 Sony data breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches' (2012) 40 Washington University Journal of Law & Policy 257

Booth R, Bastable G and Yeo N, *Money Laundering Law and Regulation: A Practical Guide* (OUP Oxford 2011)

Borne G, *A Framework for Sustainable Global Development and the Effective Governance of Risk* (Edwin Mellen Press 2010)

Bosch R and Bösch R, *Banking Regulation: Jurisdictional Comparisons* (Thomson Reuters 2012)

Bossong R and Wagner B, 'A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union' in Bures O and Carrapico H (eds), *Security Privatization* (Springer 2018)

Bradbury JA, 'The policy implications of differing concepts of risk' (1989) 14 Science, Technology, & Human Values 380

Braithwaite J, 'Enforced self-regulation: A new strategy for corporate crime control' (1982) 80 Michigan law review 1466

Brass D and others, *Contemporary perspectives on organizational social networks* (Emerald Group Publishing 2014)

Brenner SW, 'Cybercrime investigation and prosecution: The role of penal and procedural law' (2001) 8.2 eLaw Journal: Murdoch University Electronic Journal of Law 1

Brenner SW, 'Toward a criminal law for cyberspace: A new model of law enforcement' (2004) 30 Rutgers Computer & Tech LJ 1

Bridges L, 'The changing face of malware' (2008) 1 Network Security 17

Brooke GT, 'Uncertainty, Profit and Entrepreneurial Action: Frank Knight's Contribution Reconsidered' (2010) 32 Journal of the History of Economic Thought (Cambridge University Press)

Bruinsma G, Elffers H and De Keijser J, *Punishment, Places and Perpetrators* (Routledge 2012)

Burkart P and McCourt T, *Why Hackers Win: Power and Disruption in the Network Society* (University of California Press 2019)

Börzel TA, 'Governance with/out Government' (2010) False promises or flawed premises

Calliess C and Baumgarten A, 'Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective' (2020) 21 German Law Journal 1149

Camillo M, 'Cybersecurity: Risks and management of risks for global banks and financial institutions' (2017) 10 Journal of Risk Management in Financial Institutions 196

Campbell S and Currie G, 'Against Beck: In defence of risk analysis' (2006) 36 Philosophy of the Social Sciences 149

Cannon DL, *CISA Certified Information Systems Auditor Study Guide* (Wiley 2009)

Carey M and Stulz RM, *The Risks of Financial Institutions* (National Bureau of Economic Research 2005)

Carlsmith KM, Darley JM and Robinson PH, 'Why do we punish? Deterrence and just deserts as motives for punishment' (2002) 83 Journal of personality and social psychology 284

Carnell RS and others, *The law of financial institutions* (Lippincott Williams & Wilkins 2021)

Carrapico H and Farrand B, ''Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers' (2017) 67 Crime, Law and social change 245

Carrapico HF and others, 'Disputing security and risk: The convoluted politics of uncertainty', *The Politics of Uncertainty* (Routledge 2020)

Centre TR and Forum IT, *ITF Round Tables Port Competition and Hinterland Connections*, vol 143 (Organization for Economic 2009)

Chayes S, *Thieves of State: Why Corruption Threatens Global Security* (W. W. Norton 2015)

Chiu IHY, *Regulatory Convergence in EU Securities Regulation* (Wolters Kluwer 2008)

Christiansen B and Piekarz A, *Global Cyber Security Labor Shortage and International Business Risk* (IGI Global 2018)

Clarke L and Short Jr JF, 'Social organization and risk: Some current controversies' (1993) 19 Annual Review of Sociology 375

Clough J, *The Council of Europe Convention on cybercrime: definingcrime'in a digital world* (Springer 2012)

Coburn A, Leverett E and Woo G, *Solving Cyber Risk: Protecting Your Company and Society* (Wiley 2018)

Comizio VG, Dayanim B and Bain L, 'Cybersecurity as a global concern in need of global solutions: an overview of financial regulatory developments in 2015' (2016) 17 Journal of Investment Compliance 101

Committee GBPHCES and Cash W, *Fortieth report of session 2012-13: documents considered by the Committee on 24 April 2013, including the following recommendations for debate,*

adjustment of direct farm payments for 2013; enhanced cooperation and financial transaction tax; 2013 General Budget, report, together with formal minutes (Stationery Office 2013)

Committee GBPHoCT and Tyrie A, *Financial Conduct Authority: twenty-sixth report of session 2010-12, report, together with formal minutes, oral and written evidence* (Stationery Office 2012)

Conti-Brown P, 'The Institution of Federal Reserve Independence' (2015) 32 Yale Journal on Regulation 257

Cosgrave JF, *The sociology of risk and gambling reader* (Taylor & Francis 2006)

Covello VT and others, *Uncertainty in risk assessment, risk management, and decision making*, vol 4 (Springer Science & Business Media 2013)

Crisanto JC and Prenio J, 'Regulatory approaches to enhance banks' cybersecurity frameworks' (2017) Financial Stability Institutions (FSI) Insights on policy implementation

Cunliffe AL and Jun JS, 'The need for reflexivity in public administration' (2005) 37 Administration & society 225

Day JM, *Crime, values, and religion* (Greenwood Publishing Group 1987)

de Arimatéia da Cruz J, 'The Legislative Framework of the European Union (EU) Convention on Cybercrime' (2020) The Palgrave Handbook of International Cybercrime and Cyberdeviance 223

De Bruin R and Von Solms S, *Cybersecurity Governance: How can we measure it?* (IEEE 2016)

de Capitani di Vimercati S, Samarati P and Katsikas S, *Security and Privacy in the Age of Uncertainty: IFIP TC11 18th International Conference on Information Security (SEC2003) May 26–28, 2003, Athens, Greece* (Springer US 2013)

Decrop A, 'Triangulation in qualitative tourism research' (1999) 20 Tourism management 157

Department IMFWH, *United States: 2019 Article IV Consultation - Press Release; Staff Report; and Statement by the Executive Director for the United States* (INTERNATIONAL MONETARY FUND 2019)

Didenko AN, 'Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond' (2020) 25 Uniform Law Review 125

Dieleman H, 'Sustainability, art and reflexivity' (2008) 108 Sustainability: A new frontier for the arts and cultures 146

Dignan J, *Understanding victims and restorative justice* (McGraw-Hill Education (UK) 2004)

Dimsdale NH and Hotson A, *British Financial Crises Since 1825* (Oxford University Press 2014)

Dionne G, Chun OM and Triki T, 'The governance of risk management: The importance of directors' independence and financial knowledge' (2019) 22 Risk Management and Insurance Review 247

Duff A and Duff RA, *Punishment, communication, and community* (Oxford University Press, USA 2001)

Dunn-Cavelty M and Suter M, 'Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection' (2009) 2 International Journal of Critical Infrastructure Protection 179

Ellis R and Mohan V, *Rewired: Cybersecurity Governance* (Wiley 2019)

Ellul A and Yerramilli V, 'Stronger risk controls, lower risk: Evidence from US bank holding companies' (2013) 68 The Journal of Finance 1757

Emezue G, Kosch I and Kangel M, *Justice and Human Dignity in Africa* (Lulu 2014)

Fadayo M, 'An examination of e-banking fraud prevention and detection in Nigerian banks' (De Montfort University 2018)

Falola T and Adebayo AG, *Culture, Politics and Money Among the Yoruba* (Transaction Publishers)

Farrand B, '"Alone we can do so little; together we can do so much": the essential role of EU agencies in combatting the sale of counterfeit goods' (2019) 28 European Security 22

Farrand B, 'Managing security uncertainty with emerging technologies: the example of the governance of neuroprosthetic research' in Calcara A, Csernatoni R and Lavallée C (eds), *Emerging Security Technologies and EU Governance: Actors, Practices and Processes* (1st edn, Routledge 2020)

Feinberg J, 'Collective Responsibility' (1968) 65 The Journal of Philosophy 674

Feindt PH and Weiland S, 'Reflexive governance: exploring the concept and assessing its critical potential for sustainable development. Introduction to the special issue' (2018) 20 Journal of Environmental Policy & Planning 661

Feng CQ and Wang T, 'Does CIO risk appetite matter? Evidence from information security breach incidents' (2019) 32 International Journal of Accounting Information Systems 59

Ferran E, 'The break-up of the financial services authority' (2011) 31 Oxford Journal of Legal Studies 455

Fields Z, *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution* (IGI Global 2018)

Fisher JD, *Fighting fraud and financial crime: a new architecture for the investigation and prosecution of serious fraud, corruption and financial market crimes* (Policy Exchange 2010)

Fisse B, 'The attribution of criminal liability to corporations: A statutory model' (1991) 13 Sydney Law Review 277

Fisse B and Braithwaite J, 'The allocation of responsibility for corporate crime: Individualism, collectivism and accountability' (1986) 11 Sydney Law Review 468

Freese J and Peterson D, 'Replication in social science' (2017) 43 Annual Review of Sociology 147

Friedman J and Posner R, *What caused the financial crisis* (University of Pennsylvania Press 2011)

Fulea DC and Corbu MC, *Crime in Cyberspace: Approaches on Legislative Regulation in the Field of Cybercrime* ("Carol I" National Defence University 2014)

Fund IM, *United Kingdom: Financial Sector Assessment Program-Financial System Stability Assessment* (International Monetary Fund 2016)

Gaidosch T and others, *Cybersecurity risk supervision* (International Monetary Fund 2019)

Gallaher MP, Link AN and Rowe B, *Cyber Security: Economic Strategies and Public Policy Alternatives* (Edward Elgar Publishing, Incorporated 2008)

Galligan D, *Law in modern society* (OUP Oxford 2006)

Garrett GA, *Cybersecurity in the Digital Age: Tools, Techniques, & Best Practices* (Wolters Kluwer Law & Business 2018)

Garrison C and Hamilton C, 'A comparative analysis of the EU GDPR to the US's breach notifications' (2019) 28 Information & Communications Technology Law 99

Gehem M and others, *Assessing Cyber Security: A meta analysis of threats, trends, and responses to cyber attacks* (The Hague Centre for Strategic Studies 2015)

Gerber MM and Jackson J, 'Retribution as revenge and retribution as just deserts' (2013) 26 Social Justice Research 61

Gercke M, *Europe's legal approaches to cybercrime* (Springer 2009)

Geyer F and van der Zouwen J, *Sociocybernetic Paradoxes: observation, control and evolution of self-steering systems* (Sage 1986)

Giddens A, *Modernity and Self-identity: Self and Society in the Late Modern Age* (Stanford University Press 1991)

Godwin A, Howse T and Ramsay I, 'A Jurisdictional Comparison of the Twin Peaks Model of Financial Regulation' (2017) 18 *Journal of Banking Regulation* 103

Gonzalez R, Llopis J and Gasco J, 'Information technology outsourcing in financial services' (2013) 33 The Service Industries Journal 909

Gordon S and Ford R, 'On the definition and classification of cybercrime' (2006) 2 Journal in Computer Virology 13

Gotterbarn D, *Computer ethics: Responsibility regained* (Honor Society of Phi Kappa Phi 1991)

Gottesman A and Leibrock M, *Understanding Systemic Risk in Global Financial Markets* (Wiley 2017)

Gottschalk P, 'Categories of financial crime' (2010) 17 Journal of Financial Crime 441

Gouldson A and Murphy J, *Regulatory realities: The implementation and impact of industrial environmental regulation* (Routledge 2013)

Griggs G and Gul S, 'Cybersecurity threats: What retirement plan sponsors and fiduciaries need to know—and do' (2017) 24 Journal of Pension Benefits: Issues in Administration 17

Gritzalis S and others, *Trust, Privacy and Security in Digital Business* (Lecture Notes in Computer Science 2019)

Guinchard A, 'Between hype and understatement: reassessing cyber risks as a security strategy' (2011) 4 Journal of Strategic Security 75

Haimes YY and Sage AP, *Risk Modeling, Assessment, and Management* (Wiley 2015)

Haller J and Wallen C, *Managing third party risk in financial services organizations: a resilience-based approach* (Carnegie Mellon University Software Engineering Institute September 2016)

Hamid J, Gianluigi M and Lilburn WD, *Handbook Of Electronic Security And Digital Forensics* (World Scientific Publishing Company 2010)

Haruna MA, 'Analysis of value creation of electronic banking in Nigeria' (2012) 46 International Journal of Advanced Research in IT and Engineering, 1 (2), 29

Hassan AB, Lass FD and Makinde J, 'Cybercrime in Nigeria: causes, effects and the way out' (2012) 2 Asian Research Publishing Network Journal of Science and Technology 626

Helleiner E and Pagliari S, 'The end of self-regulation? Hedge funds and derivatives in global financial governance' (2009) *Global Finance in Crisis: The Politics of International Regulatory Change*

Heng Y-K, *War as risk management: strategy and conflict in an age of globalised risks* (Routledge 2006)

Hesse H, *Financial intermediation in the pre-consolidated banking sector in Nigeria* (The World Bank 2007)

Hodges C, *Law and Corporate Behaviour: Integrating Theories of Regulation, Enforcement, Compliance and Ethics* (Bloomsbury Publishing 2015)

Hoffman SK and McGinley TG, *Identity theft: a reference handbook* (ABC-CLIO 2010)

Holman C and Luneburg W, 'Lobbying and transparency: A comparative analysis of regulatory reform' (2012) 1 Interest Groups & Advocacy 75

Holt TJ and Bossler AM, *Cybercrime in Progress: Theory and prevention of technology-enabled offenses* (Taylor & Francis 2015)

Hooda R, *Statistics for business and economics* (Vikas Publishing House 2013)

House USC, Services CoF and Investigations SoOa, *Oversight of the Financial Stability Oversight Council: Hearing Before the Subcommittee on Oversight and Investigations of the Committee on Financial Services, U.S. House of Representatives, One Hundred Thirteenth Congress, Second Session, September 17, 2014* (US Government Printing Office 2015)

Hutchins JP and others, *U.S. Data Breach Notification Law: State by State* (American Bar Association, Section of Science & Technology Law 2007)

Hyytiäinen P, 'Sharing cyber threat intelligence in cyber exercise: Does controlled sharing of threat intelligence improve situation awareness?' (JAMK University of Applied Sciences 2018)

Héritier A and Lehmkuhl D, 'The shadow of hierarchy and new modes of governance' (2008) 28 Journal of public policy 1

Ibrahim A and others, 'A security review of local government using NIST CSF: a case study' (2018) 74 The Journal of Supercomputing 5171

Isaacs T and Vernon R, *Accountability for collective wrongdoing* (Cambridge University Press 2011)

Jackson C, Russell S and Cowles B, *Beyond the Beltway - The Problems with NIST's Approaches to Cybersecurity and Alternatives for NSF Science* (Center for Applied Cybersecurity Research 2017)

James O, 'Regulation inside government: Public interest justifications and regulatory failures' (2000) 78 Public Administration 327

Jessop B, 'State theory, regulation, and autopoiesis: debates and controversies' (2001) 25 Capital & Class 83

Joanna G and Jenny H, *Implementing Financial Regulation-Theory and Practice* (Wiley Online Library 2016)

Job J, Stout A and Smith R, 'Culture Change in Three Taxation Administrations: From Command-and-Control to Responsive Regulation' (2007) 29 Law & Policy 84

Johnson AL, 'Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation' (2016) 20 North Carolina Banking Institute 277

Johnson KN, 'Managing cyber risks' (2015) 50 Georgia Law Review 547

Johnson KN, 'Innovating to new heists: regulating cyber threats in the financial services industry' (2017) The Most Important Concepts in Finance 28

Kaffenberger L and Kopp E, *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment* (Carnegie Endowment for International Peace 2019)

Kalkman M, 'Re-Assessing Regulation in Light of the Financial Crisis' (2010) Inter Alia 96

Karagiannopoulos V, *Living with hacktivism: From Conflict to Symbiosis* (Palgrave Studies in Cybercrime and Cybersecurity, 1st edn, Palgrave Macmillan, Cham 2018)

Karyda M and Mitrou L, *Data Breach Notification: Issues and Challenges for Security Management* (2016)

Keller N, 'Picking Up the Framework's Pace Internationally' (2019)

Kesharwani S and Mishra S, 'Cybercrime: An Emerging Threat to Banks and NBFCs' (2020) 2 Cybernomics 13

King AA and Lenox MJ, 'Industry Self-Regulation without Sanctions: The Chemical Industry's Responsible Care Program' (2000) Academy of Management Journal 698

Kleidermacher D and Kleidermacher M, *Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development* (Elsevier Science 2012)

Kleinig J and others, *Security and Privacy: Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States* (ANU E Press 2011)

Klinke A and Renn O, 'A new approach to risk evaluation and management: Risk-based, precaution-based, and discourse-based strategies' (2002) 22 Risk analysis 1071

Knight FH, *Risk, uncertainty and profit: with an additional introductory essay hitherto unpublished* (London school of economics and political science 1933)

Koop C and Lodge M, 'What is regulation? An interdisciplinary concept analysis' (2017) 11 Regulation & Governance 95

Kosseff J, *Cybersecurity Law* (Wiley 2019)

Kramer MH, *The ethics of capital punishment: A philosophical investigation of evil and its consequences* (OUP Oxford 2011)

Kriesberg SM, 'Decisionmaking models and the control of corporate crime' (1976) 85 Yale Law Journal 1091

Kshetri N, *Cybercrime and Cybersecurity in the Global South* (Palgrave Macmillan UK 2013)

Kuerbis B and Badiei F, 'Mapping the cybersecurity institutional landscape' (2017) 19 Digital Policy, Regulation and Governance 466

Kuhlmann S, Stegmaier P and Konrad K, 'The tentative governance of emerging science and technology—A conceptual introduction' (2019) 48 Research policy 1091

Kurosu M, *Human-Computer Interaction. Interaction Contexts: 19th International Conference, HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings* (Springer International Publishing 2017)

Kwon J and Johnson ME, *An Organizational Learning Perspective on Proactive vs. Reactive investment in Information Security* (Citeseer 2011)

Labra O and others (eds), *Thematic analysis in social work: A case study* (Global Social Work-Cutting Edge Issues and Critical Reflections, Books on Demand 2019)

Lagazio M, Sherif N and Cushman M, 'A multi-level approach to understanding the impact of cyber crime on the financial sector' (2014) 45 Computers & Security 58

Laleh N and Azgomi MA (eds), *A taxonomy of frauds and fraud detection techniques*, vol 31 (Information Systems, Technology and Management ICISTM 2009 Communications in Computer and Information Science, Springer 2009)

Langevoort DC, 'Monitoring: The behavorial economics of corporate compliance with law' (2002) Columbia Business Law Review 71

Leondes CT, *Database and Data Communication Network Systems, Three-Volume Set: Techniques and Applications* (Elsevier Science 2002)

Li X, 'Taxonomy of Cybercrime' (2016) 1 Journal of Legal Studies 1

List C and Pettit P, *Group agency: The possibility, design, and status of corporate agents* (Oxford University Press 2011)

Liu J, Hebenton B and Jou S, *Handbook of Asian criminology* (Springer 2013)

Lyle C, 'Lobbying: An Overview and Outlook' (2020) Metamorphosis 1

MacDonald JW, 'Classification of Crimes' (1932) 18 Cornell Law Quarterly 524

MacHugh GA, 'Christian faith and criminal justice: Toward a Christian response to crime and punishment' (1978)

Majone G, 'The rise of the regulatory state in Europe' (1994) 17 West European Politics 77

Majone G, 'From the positive to the regulatory state: Causes and consequences of changes in the mode of governance' (1997) 17 Journal of public policy 139

Malhotra Y, *Beyond Model Risk Management to Model Risk Arbitrage for FinTech Era: How to Navigate 'Uncertainty'... When 'Models' Are 'Wrong'... And Knowledge'...'Imperfect'! Knight Reconsidered Again: Risk, Uncertainty, & Profit Beyond ZIRP & NIRP* (Princeton Quant Trading Conference, Princeton University 16 April 2016)

Management Association IR, *National Security: Breakthroughs in Research and Practice: Breakthroughs in Research and Practice* (IGI Global 2019)

Marcus DJ, 'The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information' (2018) 68 Duke Law Journal 555

Markandya A and Nations FaAOotU, *Policies for Sustainable Development: Four Essays* (Food and Agriculture Organization of the United Nations 1994)

Martin A and San Juan V, 'Cyber governance and the financial services sector: The role of public-private partnerships' (2019) Rewired 97

Maurer T, Levite A and Perkovich G, 'Toward a global norm against manipulating the integrity of financial data' (2017) Economics Discussion Papers

Mawere M and Awuah-Nyamekye S, *Harnessing Cultural Capital for Sustainability: A Pan Africanist Perspective* (Langaa RPCIG 2015)

Mayntz R, *Negotiated reform: The multilevel governance of financial regulation*, vol 85 (Campus Verlag 2015)

McAdams JB, 'The appropriate sanctions for corporate criminal liability: An eclectic alternative' (1977) 46 University of Cincinnati Law Review 989

McPhail TL and Phipps S, *Global Communication: Theories, Stakeholders, and Trends* (Wiley 2019)

Meadowcroft J and Steurer R, 'Assessment practices in the policy and politics cycles: a contribution to reflexive governance for sustainable development?' (2018) 20 Journal of environmental policy & planning 734

Meier RF, 'Perspectives on the concept of social control' (1982) 8 Annual Review of Sociology 35

Mellema G, *Collective responsibility*, vol 50 (Rodopi 1997)

Merton RC, 'Financial innovation and the management and regulation of financial institutions' (1995) 19 Journal of Banking & Finance 461

Mohammed F, 'Impact of Corporate governance on Banking Sector performance in Nigeria' (2011) 2 International Journal of Economic Development Research and Investment 52

Mokhiber R, *Corporate Crime and Violence: Big Business Power and the Abuse of the Public Trust* (Sierra Club Books 1988)

Molinuevo M and Sez S, *Regulatory assessment toolkit: A practical methodology for assessing regulation on trade and investment in services* (World Bank Publications 2014)

Monetary IMF and Department CM, *United States: Financial Sector Assessment Program-Detailed Assessment of Observance on the Basel Core Principles for Effective Banking Supervision* (International Monetary Fund 2015)

Mongiardino A and Plath C, 'Risk governance at large banks: Have any lessons been learned?' (2010) 3 Journal of Risk Management in Financial Institutions 116

Morgan B and Yeung K, *An introduction to law and regulation: Text and materials* (Cambridge University Press 2007)

Murray A, 'Symbiotic Regulation' (2008) 26 The John Marshall Journal of Information Technology & Privacy Law 207

Nabi SI and others, 'Data confidentiality and integrity issues and role of information security management standard, policies and practices–An empirical study of telecommunication industry in Pakistan', *Security Technology, Disaster Recovery and Business Continuity* (Springer 2010)

Najera-Gutierrez G and Ansari JA, *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux, 3rd Edition* (Packt Publishing 2018)

Narain A, Ötker MI and Pazarbasioglu C, *Building a more resilient financial sector: Reforms in the wake of the global crisis* (International Monetary Fund 2012)

Nayak U and Rao UH, *The InfoSec Handbook: An Introduction to Information Security* (Apress 2014)

Nelson M, *Guide to the Presidency* (Taylor & Francis 2015)

Ngwu FN, Osuji OK and Stephen FH, *Corporate Governance in Developing and Emerging Markets* (Taylor & Francis 2016)

O'Donovan J, *Lender Liability* (Sweet & Maxwell 2005)

Obuah E, 'Combating corruption in a “failed” state: the Nigerian Economic and Financial Crimes Commission (EFCC)' (2010) 12 Journal of Sustainable Development in Africa 27

Ochieng PA, 'An analysis of the strengths and limitation of qualitative and quantitative research paradigms' (2009) 13 Problems of Education in the 21st Century 13

OECD, *Enhancing the Role of Insurance in Cyber Risk Management* (OECD Publishing 2017)

OECD, 'Lobbying in the 21st Century: Transparency, Integrity and Access' (2021)

Okonjo-Iweala N, *Reforming the unreformable: Lessons from Nigeria* (Mit Press 2014)

Okpara GC, 'Bank reforms and the performance of the Nigerian banking sector: An empirical analysis' (2011) 2 International Journal of Current Research 142

Olaniyan K, *Corruption and Human Rights Law in Africa* (Bloomsbury Publishing 2014)

Olayemi OJ, 'A socio-technological analysis of cybercrime and cyber security in Nigeria' (2014) 6 International Journal of Sociology and Anthropology 116

Omankhanlen AE and Taiwo J, 'The role of corporate governance in the growth of Nigerian banks' (2013) 1 Journal of Business law and Ethics 44

Omotubora AO, 'Comparative perspectives on cybercrime legislation in Nigeria and the UK - a case for revisiting the "hacking" offences under the Nigerian Cybercrime Act 2015' (2016) 7 European Journal of Law and Technology 1

Onamson FO, *Law and Creditor Protection in Nigeria* (Malthouse Press 2017)

Onyema E and others, 'The Economic and Financial Crimes Commission and the politics of (in) effective implementation of Nigeria’s anti-corruption policy' (2018)

Orji UJ, 'Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria' (2019) 24 Tilburg Law Review

Overly MR and Karlyn MA, *A Guide to IT Contracting: Checklists, Tools, and Techniques* (CRC Press 2012)

Parker C and Development OfEC-oa, *Reducing the risk of policy failure: challenges for regulatory compliance : final version* (OECD 2000)

Paseda O, 'Banking regulation in Nigeria: A review article' (2012) 25 International Organization of Scientific Research Journal of Humanities and Social Sciences 38

Patton MQ, 'Enhancing the quality and credibility of qualitative analysis' (1999) 34 Health services research 1189

Pawlak P and Barmpaliou P-N, 'Politics of cybersecurity capacity building: conundrum and opportunity' (2017) 2 Journal of Cyber Policy 123

Peltier TR, *Information Security Policies and Procedures: A Practitioner's Reference, Second Edition* (Taylor & Francis 2004)

Peta C, 'Cyber-Security-Current Topic of National Security (I)' (2013) 2 Studii de Securitate Publica 66

Pickett KS and Pickett JM, *Financial crime investigation and control* (John Wiley & Sons 2002)

Pillow W, 'Confession, catharsis, or cure? Rethinking the uses of reflexivity as methodological power in qualitative research' (2003) 16 International journal of qualitative studies in education 175

Pomerleau P-L and Lowery DL, 'Conclusions and Implications for Practice and Future Studies on Public–Private Partnerships', *Countering Cyber Threats to Financial Institutions* (Springer 2020)

Pomerleau P-L and Lowery DL, 'Major Themes in the Literature of Cybersecurity and Public–Private Partnerships; A Focus on Financial Institutions' (2020) Countering Cyber Threats to Financial Institutions 87

Porcedda MG, 'Regulation of Data Breaches in the European Union: Private Companies in the Driver's Seat of Cybersecurity?' in Bures O and Carrapico H (eds), *Security Privatization: How Non-security-related Private Businesses Shape Security Governance* (Springer International Publishing 2018)

Priest M, 'The privatization of regulation: five models of self-regulation' (1997) 29 Ottawa Law Review 233

QC CN and others, *Corruption and Misuse of Public Office* (OUP Oxford 2011)

Rakoff TD, 'The Choice Between Formal and Informal Modes of Administrative Regulation' (2000) Administrative Law Review 159

Reaz M and Arun T, 'Corporate governance in developing economies: perspective from the banking sector in Bangladesh' (2006) 7 Journal of Banking Regulation 94

Renn O, 'Concepts of risk: a classification' (1992)

Renn O, 'Three decades of risk research: accomplishments and new challenges' (1998) 1 Journal of risk research 49

Renn O, *Risk governance: coping with uncertainty in a complex world* (Routledge 2017)

Rezaee Z and others, *Business Sustainability in Asia: Compliance, Performance, and Integrated Reporting and Assurance* (Wiley 2019)

Richet JL, *Cybersecurity Policies and Strategies for Cyberwarfare Prevention* (IGI Global 2015)

Rogers MK, 'The psyche of cybercriminals: A psycho-social perspective', *Cybercrimes: A Multidisciplinary Analysis* (Springer 2011)

Rogowski R, 'The emergence of reflexive global labour law' (2015) 22 Industrielle Beziehungen/The German Journal of Industrial Relations 72

Rorie ML and Wellford CF, *The Handbook of White-Collar Crime* (Wiley 2019)

Rumsfeld D, *Department of Defense News Briefing - Secretary Rumsfeld and Gen. Myers* (US Department of Defense 2002)

Rustad ML, 'Private enforcement of cybercrime on the electronic frontier' (2001) 11 Southern California Interdisciplinary Law Journal 63

Ryan T, *Managing crisis and risk in mental health nursing* (Nelson Thornes 1999)

Råman J, *Regulating Secure Software Development: analysing the potential regulatory solutions for the lack of security in software*, vol 102 (Lapland University Press 2006)

Salawu A and Owolabi TOS, *Exploring Journalism Practice and Perception in Developing Countries* (IGI Global 2017)

Sanusi L, 'The Nigerian Banking Industry: what went wrong and the way forward' (2010) 3 Delivered at Annual Convocation Ceremony of Bayero University, Kano held on 2010

Saxegaard M and Department IMFA, *Excess Liquidity and the Effectiveness of Monetary Policy: Evidence from Sub-Saharan Africa* (INTERNATIONAL MONETARY FUND 2006)

Schjolberg S, 'The history of global harmonization on cybercrime legislation–the road to geneva' (2008) 1 Journal of international commercial law and technology 1

Schumacher P, *The Autopoiesis of Architecture, Volume I: A New Framework for Architecture* (Autopoiesis of architecture, Wiley 2011)

Selznick P, 'Focusing organizational research on regulation' (1985) 1 Regulatory policy and the social sciences 363

Serkin G, *Frontier: Exploring the Top Ten Emerging Markets of Tomorrow* (Wiley 2015)

Services EMCE, *Information Storage and Management: Storing, Managing, and Protecting Digital Information in Classic, Virtualized, and Cloud Environments* (Wiley 2012)

Sesan G, Soremi B and Bankole O, 'Economic cost of cybercrime in Nigeria' (2013) Cyber Stewards Network Project, Munk School of global affairs, University of Toronto

Shirreff D, *Dealing with financial risk*, vol 41 (UNC Press Books 2004)

Simon MK and Goes J, 'Assumptions, limitations, delimitations, and scope of the study' (2013) Dissertation and Scholarly Research: Recipes for Success

Sinclair D, 'Self-regulation versus command and control? Beyond false dichotomies' (1997) 19 Law & Policy 529

Slovic P, 'The risk game' (1998) 59 Reliability engineering & system safety 73

Smiley M, 'Collective responsibility' (2005)

Smith DK, 'What Is Regulation-A Reply to Julia Black' (2002) 27 Australian Journal of Legal Philosophy 37

Sood AK, Zeadally S and Enbody RJ, 'An empirical study of HTTP-based financial botnets' (2014) 13 IEEE Transactions on Dependable and Secure Computing 236

Stirling A, 'Precaution, foresight and sustainability. Reflection and reflexivity in the governance of science and technology' (2006) Reflexive governance for sustainable development Cheltenham: Elgar 225

Stirling PA, *On Science and Precaution in the Management of Technological Risk: Volume II-case studies*, 1999)

Sudjianto A and others, 'Statistical methods for fighting financial crimes' (2010) 52 Technometrics 5

Tardzer CSK, *My Odyssey, My Country* (Xlibris US 2012)

Tayo-Tiwo AA, 'Nigerian Banks' Compliance with the Code of Corporate Governance' (Walden University (2018)

Terrell W. Herzig MCE, *Information Security in Healthcare: Managing Risk* (Healthcare Information and Management Systems Society 2010)

Teubner G, 'Substantive and reflexive elements in modern law' (1983) Law and society review 239

Tierney K, 'Toward a Critical Sociology of Risk' (1999) 14 Sociological Forum 215

Tonry M, 'Proportionality Theory in Punishment Philosophy: Fated for the Dustbin of Otiosity?' (2019) *Of One-eyed and Toothless Miscreants: Making the Punishment Fit the Crime*

Trim P and Lee YI, *Cyber Security Management: A Governance, Risk and Compliance Framework* (Taylor & Francis 2016)

Tropina T and Callanan C, *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security* (Springer International Publishing 2015)

Tupa J, Simota J and Steiner F, 'Aspects of risk management implementation for Industry 4.0' (2017) 11 Procedia Manufacturing 1223

Uche CU, 'Banking regulation in an era of structural adjustment: The case of Nigeria' (2000) Journal of Financial Regulation and compliance

Ula M, Ismail Z and Sidek ZM, 'A Framework for the governance of information security in banking system' (2011) 2011 Journal of Information Assurance & Cyber Security 1

Umar I, Samsudin RS and Mohamed Mb, 'Ascertaining the effectiveness of Economic and Financial Crimes Commission (EFCC) in tackling corruptions in Nigeria' (2018) 25 Journal of Financial Crime 658

Usman AK, 'An investigation into the critical success factors for e-banking frauds prevention in Nigeria' (University of Central Lancashire (2018)

Uzokwe HC, 'Consumer protection in the banking sector: the need for reform to protect bank consumers in Nigeria' (Brunel University London (2017)

Van Brunschot EG and Kennedy LW, *Risk Balance and Security* (SAGE Publications 2007)

van der Hof S and others, *Sweetie 2.0: Using Artificial Intelligence to Fight Webcam Child Sex Tourism* (T.M.C. Asser Press 2019)

van Willigenburg T, 'Restorative justice as empowerment: how to better serve the goals of punitive retribution' (2018) 1 International Journal of Restorative Justice 274

von Hirsch A, 'Proportionality in the philosophy of punishment: From “why punish?” to “how much?”" (1990) 1 Criminal Law Forum 259

Von Hirsch A, 'Proportionality in the Philosophy of Punishment' (1992) 16 Crime and Justice 55

Wall D, *Cybercrime: The transformation of crime in the information age*, vol 4 (Polity 2007)

Wall DS, 'The Internet as a conduit for criminal activity' in Pattavina A (ed), *Information technology and the criminal justice system* (2005/15)

Wall DS, 'Policing cybercrimes: Situating the public police in networks of security within cyberspace' (2007) 8 Police Practice and Research 183

Walters GD, *Foundations of Criminal Science: The development of knowledge*, vol 1 (Greenwood Publishing Group 1992)

Wang V, Nnaji H and Jung J, 'Internet banking in Nigeria: Cyber security breaches, practices and capability' (2020) 62 International Journal of Law, Crime and Justice 100415

Weber AM, 'The Council of Europe's Convention on Cybercrime' (2003) 18 Berkeley technology law journal 425

Weimer M and Marin L, 'The role of law in managing the tension between risk and innovation: Introduction to the special issue on regulating new and emerging technologies' (2016) 7 European journal of risk regulation 469

Winter SG and Szulanski G, 'Replication as strategy' (2001) 12 Organization science 730

Wringe B, 'Collective agents and communicative theories of punishment' (2012) 43 Journal of Social Philosophy 436

Yovits MC, *Advances in Computers* (Elsevier Science 1994)

Yusuf I and Ekundayo D, 'Regulatory non-compliance and performance of deposit money banks in Nigeria' (2018) 26 Journal of Financial Regulation and Compliance 425

Zimmerman R, 'The management of risk', *Risk evaluation and management* (Springer 1986)

Zumbansen P, 'Law after the welfare state: Formalism, functionalism, and the ironic turn of reflexive law' (2008) 56 The American Journal of Comparative Law 769

Legislation and International Legal Instruments

UK Legislation

Computer Misuse Act 1990

Data Protection Act 2018

Financial Services and Markets Act 2000

Financial Services Act 2012

Fraud Act 2006

Network and Information Systems Regulations 2018

Payment Services Regulations 2017

US Legislation

Bank Service Company Act 1962

California Civil Code 1798.82

California Online Privacy Protection Act 2003

Computer Fraud and Abuse Act 1986

Cybersecurity Information Sharing Act 2015

Fair and Accurate Credit Transactions Act 2003

Federal Deposit Insurance Act 1950

Financial Institutions Regulatory and Interest Rate Control Act of 1978

Gramm-Leach-Bliley Act 1999

New York Department of Financial Services Cybersecurity Regulation (23 NYCRR 500)

Payment Systems and Electronic Fund Transfers Act 2007

Personal Data Notification and Protection Act of 2017

Personal Data Protection and Breach Accountability Act of 2014

Sarbanes-Oxley Act 2002

Nigerian Legislation

Central Bank of Nigeria Act 2007

Cybercrimes Act 2015

Advance fee Fraud and other Fraud Related Offences Act 2006

Constitution of the Federal Republic of Nigeria 1999

Economic and Financial Crimes Commission Act 2004

Money Laundering Prohibition Act 2011

Nigerian Data Protection Regulations 2019

Nigerian Deposit Insurance Corporation 2006

EU Legislation

Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

International Legal Instruments

Council of Europe Convention on Cybercrime (ETS No. 185)

Online Sources

Accenture, 'The Cost of Cybercrime - Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection' (2019) <https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50> accessed 27 January 2020

Adeyemi Adepetun, 'Nigerian banks spent N200b preventing cyberattacks in 2019' (*TheGuardian*, 9 January 2020) <https://guardian.ng/business-services/nigerian-banks-spent-n200b-preventing-cyber-attacks-in-2019/> accessed 13 January 2021

AELEX, 'Nigeria: The Evolution Of Cyber Security In The Nigerian Banking Sector' (*Mondaq*, 16 April 2019) <https://www.mondaq.com/Nigeria/Technology/799360/The-Evolution-Of-Cyber-Security-In-The-Nigerian-Banking-Sector> accessed 5 June 2020

Alston & Bird, Cyber Alert, 'The Cybersecurity Information Sharing Act Is Now Law' 1 (23 December 2015) <https://www.alston.com/-/media/files/insights/publications/2015/12/icyber-alerti-the-cybersecurity-information-sharin/files/view-alert-as-pdf/fileattachment/15443cybersecurityinformationsharingact.pdf> accessed 10 December 2020

Bank for International Settlements, 'Guidance on cyber resilience for financial market infrastructures' (29 June 2016) <https://www.bis.org/cpmi/publ/d146.pdf> accessed 15 August 2018

Bank of America Corporation, 'Annual Report 2019' 43 <http://investor.bankofamerica.com/annual-reports-proxy-statements/2019_Annual_Report> accessed 18 July 2020

Bank of England, 'Building operational resilience: Impact tolerances for important business services' (5 December 2019) para 1.13 <https://www.bankofengland.co.uk/-

/media/boe/files/prudential-regulation/consultation-paper/2019/building-operational-resilience-impact-tolerances-for-important-business-services.pdf?la=en&hash=DAD20B3E08876E418863D37A242214BB1F32FE0A> accessed 4 August 2019

Bank of England, 'CBEST Intelligence-Led Testing: An Introduction to Cyber Threat Modelling' *Version 2.0* (2016) 19 <http://www.bankofengland.co.uk/financialstability/fsc/Documents/anintroductiontocbest.pdf > accessed 15 September 2017

Bank of England, 'Discussion Paper 01/18: Building the UK financial sector's operational resilience' (July 2018) 13 <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf?la=en&hash=4238F3B14D839EBE6BEFBD6B5E5634FB95197D8A> accessed 8 August 2019

Bank of England, 'Financial Policy Committee' <http://www.bankofengland.co.uk/financialstability/Pages/fpc/default.aspx> accessed 8 September 2017

Bank of England, Financial Stability Report Issue 37 (July 2015) <https://www.bankofengland.co.uk/-/media/boe/files/financial-stability-report/2015/july-2015.pdf> accessed 28 December 2020

Bank of England, 'Financial Stability Report (Issue No. 41)' (June 2018) 40 <https://www.bankofengland.co.uk/-/media/boe/files/financial-stability-report/2018/june-2018.pdf> accessed 19 August 2019

Bank of England, Financial Stability Report Issue No 45 (July 2019) <https://www.bankofengland.co.uk/-/media/boe/files/financial-stability-report/2019/july-2019.pdf?la=en&hash=976688AB50462983447A8908BE079743A3E3905F> accessed 26 December 2020

Bank of England, 'Memorandum of Understanding: Between the Financial Conduct Authority and the Bank of England (exercising its prudential regulation functions)' (July 2019) para 10 <https://www.bankofengland.co.uk/-/media/boe/files/memoranda-of-understanding/fca-and-

bank-prudential-july-2019.pdf?la=en&hash=8DE71C08C48852C15DB5A999A74B95D48B507F16> accessed 4 August 2019

Bank of England, 'PRA Rulebook' Rule 2 <http://www.prarulebook.co.uk/rulebook/Content/Part/214136/15-08-2019> accessed 10 August 2019

Bank of England, 'Prudential Regulation Authority: Fundamental Rules and Principles for Businesses' <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/new-bank/fundamentalruleprinciples> accessed 9 August 2019

Bank of England, R. Raphael & Sons plc – Final Notice (29 May 2019) <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/regulatory-action/r-raphael-and-sons-plc-final-notice-may-2019.pdf?la=en&hash=CA2EDBA1E3FA560F6E22BA13C8B7CBA8676B1FA4> accessed 31 December 2020

Bank of England, 'Systemic Risk Survey Results - 2019 H1' (11 July 2019) <https://www.bankofengland.co.uk/systemic-risk-survey/2019/2019-h1> accessed 9 August 2019

Bank of England, Systemic Risk Survey Results - 2019 H2 (16 December 2019) <https://www.bankofengland.co.uk/systemic-risk-survey/2019/2019-h2> accessed 31 December 2020

Bank of England, 'The Promise of FinTech – Something New Under the Sun?' (25 January 2017) <https://www.bis.org/review/r170126b.pdf> accessed 5 March 2018

Bank of England's Written Evidence to Wilson Committee in connexion with Stage Two of its Enquiry: 'Regulation in the City and the Bank of England's role', QB (1978) Q3, p 382 < https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/1978/regulation-in-the-city-and-the-boes-role.pdf?la=en&hash=4AB1C0C821A0FE0A166A07B1B13D2EB654CF9C0A> accessed 3 March 2020.

Barclays Plc, '2018 Annual Report' 57 <https://home.barclays/content/dam/home-barclays/documents/investor-relations/reports-and-events/annual-reports/2018/2018-barclays-plc-annual-report.pdf> accessed 14 August 2019

Barclays Plc, '2019 Annual Report' 57 <https://home.barclays/content/dam/home-barclays/documents/investor-relations/reports-and-events/annual-reports/2019/Barclays%20PLC%20Annual%20Report%202019.pdf> accessed 6 June 2020

Barclays PLC, 'Return to Stability - Annual Report 2015' (2015) 122 <https://www.home.barclays/content/dam/barclayspublic/docs/InvestorRelations/AnnualReports/AR2015/Barclays_PLC_Annual_Report_%202015.pdf> accessed 13 April 2018

Basel Committee on Banking Supervision, 'Compliance and Compliance Function in Banks' (April 2015) <http://www.bis.org/publ/bcbs113.pdf> accessed 10 September 2017

BofA, 'Cyber security: Insights from Bank of America's chief information security officer' (October 2019) <https://workplaceinsights.bofa.com/articles/2019/10/froelich.html> accessed 18 July 2020

BofA, 'Proxy Statement' (9 March 2020) 17 <http://investor.bankofamerica.com/static-files/599c40f7-721e-47fd-8fe1-a63a89d47532> accessed 5 July 2020

Carnegie Endowment for International Peace, 'Timeline of Cyber Incidents Involving FIs' (2020) <https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide> accessed 10 July 2020

CBN, 'A Brief of the Central Bank of Nigeria Act 2007' <https://webcache.googleusercontent.com/search?q=cache:4a0pOBKsHbEJ:https://www.cbn.gov.ng/OUT/PUBLICATIONS/PRESSRELEASE/GOV/2007/PR3-7-07.PDF+&cd=4&hl=en&ct=clnk&gl=uk> accessed 5 March 2019

CBN, 'Central Bank of Nigeria Annual Report 2017' 58 <https://www.cbn.gov.ng/Out/2018/RSD/CBN%202017%20ANNUAL%20REPORT_WEB.pdf> accessed 10 March 2019

CBN ‘Exposure draft of the Nigerian payments system risk and information security management framework’ (May 2018) <https://www.cbn.gov.ng/Out/2018/BPSD/NPS_Risk_and_Info_Sec_Mgt_Framework.pdf> accessed 12 March 2019

CBN, ‘Exposure draft of the risk-based cybersecurity framework and guidelines for deposit money banks and payment service providers’ (June 2018) Appendix I <https://www.cbn.gov.ng/Out/2018/BSD/RISK%20BASED%20CYBERSECURITY%20FRAMEWORK%20Exposure%20Draft%20June.pdf> accessed 14 March 2019

CBN, ‘Guidelines on Mobile Money Services’ (June 2015) <https://www.cbn.gov.ng/out/2015/bpsd/guidelines%20on%20mobile%20money%20services%20in%20nigeria.pdf> accessed 10 March 2019

CBN, ‘Guidelines on operations of electronic payment channels in Nigeria’ (April 2016) <https://www.cbn.gov.ng/Out/2016/BPSD/Approved%20Guidelines%20on%20Operations%20of%20Electronic%20Payment%20Channels%20in%20Nigeria.pdf> accessed 12 March 2019

CBN, ‘Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs)’ (October 2018) para 5.6 <https://www.cbn.gov.ng/Out/2018/BSD/RISK%20BASED%20CYBERSECURITY%20FRAMEWORK%20FINAL.pdf> accessed 14 March 2019

CBN, ‘The Board’ <https://www.cbn.gov.ng/AboutCBN/TheList.asp> accessed 5 March 2019

CBN, ‘The regulatory framework for Bank Verification Number (BVN) operations and watch-list for the Nigerian financial system’ (October 2017) <https://www.cbn.gov.ng/out/2017/bpsd/circular%20on%20the%20regulatory%20framework%20for%20bvn%20%20watchlist%20for%20nigerian%20financial%20system.pdf> accessed 12 March 2019

CBN, ‘The Regulatory Framework for Mobile Payment Services in Nigeria’ (November 2014)

<https://www.cbn.gov.ng/out/2014/bpsd/exposure%20draft%20regulatory%20framework%20for%20mobile%20payments%20.pdf> accessed 10 March 2019

CBN, 'The regulatory framework for the use of unstructured supplementary service data (USSD) in the Nigerian Financial System' (April 2018) <https://www.cbn.gov.ng/Out/2018/BPSD/USSD%20Regulatory%20Framework.pdf> accessed 12 March 2019

Central Bank of Nigeria, 'A Brief of the Central Bank of Nigeria Act 2007' <https://webcache.googleusercontent.com/search?q=cache:4a0pOBKsHbEJ:https://www.cbn.gov.ng/OUT/PUBLICATIONS/PRESSRELEASE/GOV/2007/PR3-7-07.PDF+&cd=4&hl=en&ct=clnk&gl=uk> accessed 5 March 2019

Central Bank of Nigeria, 'The Board' <https://www.cbn.gov.ng/AboutCBN/TheList.asp> accessed 5 March 2019

Central Bank of Nigeria (CBN), 'Understanding Monetary Policy Series No 7 - Banking Sector Reforms in Nigeria' (July 2011) 7 <https://www.cbn.gov.ng/Out/2015/MPD/UNDERSTANDING%20MONETARY%20POLICY%20SERIES%207.pdf> accessed 31 March 2019

CFPB, Consumer Data Protection Principles (2017) <https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf> accessed 10 July 2020

Chase, 'Annual Report 2019' 130 <https://www.jpmorganchase.com/corporate/investor-relations/document/annualreport-2019.pdf> accessed 1 July 2020

Chase, '2019 Proxy Statement' (6 April 2020) 68 <https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/proxy-statement2020.pdf> accessed 6 July 2020

Chase, 'Understanding Our Climate-Related Risks and Opportunities' (May 2019) 7 <www.jpmorganchase.com/corporate/Corporate-Responsibility/document/jpmc-cr-climate-report-2019.pdf> accessed 6 July 2020

Congressional Research Services, 'Financial Services and Cybersecurity: The Federal Role' (Updated 23 March 2016) 6 <https://crsreports.congress.gov/product/pdf/R/R44429> accessed 10 December 2020

Consultancy UK, 'Regulation should not crush innovation in financial services sector' (25 October 2017) <https://www.consultancy.uk/news/14262/regulation-should-not-crush-innovation-in-financial-services-sector> accessed 22 January 2018

Consumer Financial Protection Bureau (CFPB), 'Bureau Of Consumer Financial Protection v Equifax Inc: Stipulated Order For Permanent Injunction And Monetary Judgment' (23 July 2019) https://files.consumerfinance.gov/f/documents/cfpb_equifax-inc_stipulated-order_2019-07.pdf> accessed 10 December 2020

Council of Europe, 'Convention on Cybercrime (ETS No. 185) - Request by Nigeria to be invited to accede' <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680717468> accessed 15 March 2019

CRS, 'Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework' (Updated 10 March 2020) 5 <https://fas.org/sgp/crs/misc/R44918.pdf> accessed 10 July 2020

David Zaring, 'Equifax Deal: Credit Agencies Must Change How They Manage Data' (30 July 2019) <https://knowledge.wharton.upenn.edu/article/equifax-settlement-key-takeaways/> accessed 15 July 2020

Department for Digital, Culture, Media and Sport, Analysis of responses to public consultation: Security of Network and Information Systems (January 2018) 25 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677066/NIS_Consultation_Response_-_Analysis_of_Responses.pdf> accessed 12 December 2020

Department for Digital, Culture, Media and Sport, Security of Network and Information Systems Public Consultation (August 2017) 6 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf> accessed 12 December 2020

Department for Digital, Culture, Media and Sport, Security of Network and Information Systems: Government Response to Public Consultation (January 2018) 16 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf> accessed 13 December 2020

Department for Transport, Implementation of the NIS Directive DfT Guidance version 1.1 (December 2018) Para 2.4 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/892104/implementation-of-the-nis-directive-dft-guidance-document.pdf> accessed 1 November 2020

Depository and Financial Payments Survey (DFIPS) and reported in FRS 'Changes in U.S. Payments Fraud from 2012 to 2016: Evidence from the Federal Reserve Payments Study' (October 2018) 39 <https://www.federalreserve.gov/publications/files/changes-in-us-payments-fraud-from-2012-to-2016-20181016.pdf> accessed 6 July 2020

Economic and Financial Crimes Commission, EFCC Arrests Three Suspected Fraudsters for Attempted Hacking <https://efccnigeria.org/efcc/news/987-efcc-arrests-three-suspected-fraudsters-for-attempted-hacking> accessed 24 September 2020

EFCC, 'EFCC Arraigns Two Access Bank Staff for £100,000 Fraud' (25 January 2019) <https://efccnigeria.org/efcc/news/3677-efcc-arraigns-two-access-bank-staff-for-100-000-fraud> accessed 30 April 2019

EFCC, 'EFCC Arrests Three Suspected Fraudsters for Attempted Hacking' (31 August 2014) <https://efccnigeria.org/efcc/news/987-efcc-arrests-three-suspected-fraudsters-for-attempted-hacking> accessed 30 April 2019

EFCC, 'Court Jails Ex-Banker 12 years For N450m Fraud' (14 March 2018) <https://efccnigeria.org/efcc/news/3131-court-jails-ex-banker-12-years-for-n450m-fraud> accessed 29 March 2019

EFCC, 'Man Bags 29 Years for N2m Cyber Fraud' (6 May 2019) <https://efccnigeria.org/efcc/news/4184-man-bags-29-years-for-n2m-cyber-fraud-2> accessed 6 May 2019

EFCC, N466m Fraud: Fraudsters who Defrauded Polaris Bank Get N1m Bail <https://efccnigeria.org/efcc/news/3659-n466m-fraud-fraudsters-who-defrauded-polaris-bank-get-n1m-bail> accessed 24 September 2020

Eric Mogilnicki, 'CFPB has too much flexibility in assessing fines' (16 April 2019) <www.americanbanker.com/opinion/cfpb-has-too-much-flexibility-in-assessing-fines> accessed 2 August 2020

European Banking Authority, EBA/GL/2019/02 Final Report on EBA Guidelines on Outsourcing arrangements (25 February 2019) para 42 <https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1> accessed 11 February 2020

European Commission, 'Operational Guidance for the EU's international cooperation on cyber capacity building' (European Union, 2018) <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf> accessed 21 June 2019

European Union Agency for Network and Information Security, 'WannaCry Ransomware: First ever case of cyber cooperation at EU level' *Press Release* (15 May 2017) <https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level> accessed 25 July 2017

EUROPOL, 'Internet Organised Crime Threat Assessment (IOCTA)' (2020) 33 <https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf> accessed 25 May 2021

FDIC, 'Proposed Rules: Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers' Vol. 86, No. 7 (*Federal Register*, 12 January 2021) 2302 <https://www.fdic.gov/news/board/2020/2020-12-15-notice-sum-c-fr.pdf> accessed 15 January 2021

Federal Bureau of Investigation, 'Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government' <https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view> accessed 10 July 2020

Federal Deposit Insurance Corporation, 'A Framework for Cybersecurity' (2015) 8 <https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin15/si_winter2015-article01.pdf> accessed 10 October 2019

Federal Deposit Insurance Corporation, '1987 Annual Report' (24 June 1988) xiii <https://www.fdic.gov/about/strategic/report/archives/fdic-ar-1987.pdf> accessed 9 November 2018

Federal Financial Institutions Examination Council, 'Information Technology Examination Handbook' <http://ithandbook.ffiec.gov/it-booklets/information-security.aspx> accessed 20 May 2019 (FFIEC IT Examination Handbook)

Federal Reserve System, 'Advance Notice of Proposed Rulemaking - Enhanced Cyber Risk Management Standards' (19 October 2016) 27 <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20161019a1.pdf> accessed 15 August 2018

Federal Trade Commission, "FACTA Disposal Rule Goes into Effect June 1" (1 June 2005) <https://www.ftc.gov/news-events/press-releases/2005/06/facta-disposal-rule-goes-effect-june-1> accessed 21 July 2020.

FFIEC, 'Annual Report 2014' (26 March 2015) 21 <https://www.ffiec.gov/PDF/annrpt14.pdf> accessed 2 August 2018

FFIEC, 'Annual Report 2017' (30 March 2018) 27 <https://www.ffiec.gov/PDF/annrpt17.pdf> accessed 14 March 2019

FFIEC, 'Cybersecurity Resource Guide for Financial Institutions' (October 2018) <https://www.ffiec.gov/press/pdf/FFIEC%20Cybersecurity%20Resource%20Guide%20for%20Financial%20Institutions.pdf> accessed 20 May 2019

FFIEC, 'FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors' (June 2015)

<ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf> accessed 18 August 2018

FFIEC, 'FFIEC Launches Cybersecurity Web Page, Promotes Awareness of Cybersecurity Activities' (24 June 2014) <https://www.ffiec.gov/press/pr062414.htm> accessed 16 August 2018

FFIEC, 'Uniform Rating System for Information Technology' (19 October 2016) 9 <https://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers/risk-based-supervision/uniform-rating-system-for-information-technology.aspx#:~:text=The%20Agencies%20use%20the%20Uniform,financial%20institutions%20and%20their%20TSPs.&text=The%20URSIT%20is%20based%20on,Acquisition%2C%20and%20Support%20and%20Delivery.> accessed 15 July 2020

Financial Conduct Authority, 'Business Plan 2019/2020' 16 <https://www.fca.org.uk/publication/business-plans/business-plan-2019-20.pdf> accessed 4 August 2019

Financial Conduct Authority 'Cybersecurity - industry insights' (March 2019) para 2.2 <https://www.fca.org.uk/publication/research/cyber-security-industry-insights.pdf> accessed 10 August 2019

Financial Conduct Authority, Cyber Resilience (18 May 2017) <https://www.fca.org.uk/firms/cyber-resilience> accessed 4 December 2020

Financial Conduct Authority, 'Cyber and technology resilience in UK financial services' (27 November 2018) *Speeches* <https://www.fca.org.uk/news/speeches/cyber-and-technology-resilience-uk-financial-services > accessed 13 August 2019

Financial Conduct Authority, 'Cyber and Technology Resilience: Themes from cross-sector survey 2017/2018' (November 2018) para 2.4 <https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf> accessed 6 August 2019

Financial Conduct Authority, 'Decision Notice: Standard Chartered Bank 2019' (5 February 2019) <https://www.fca.org.uk/publication/decision-notices/standard-chartered-bank-2019.pdf> accessed 4 August 2019

Financial Conduct Authority, ‘Enforcement Guide’ Annex 2, para 7 <https://www.handbook.fca.org.uk/handbook/document/EG_Full_20160101.pdf> accessed 6 January 2021

Financial Conduct Authority, ‘FCA Mission: Our Approach to Supervision’ (March 2018) 11 <https://www.fca.org.uk/publication/corporate/our-approach-supervision.pdf> accessed 31 December 2020

Financial Conduct Authority, ‘FG 16/5 Guidance for firms outsourcing to the ‘cloud’ and other third-party IT services’ (July 2018) <https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf> accessed 4 August 2019

Financial Conduct Authority, ‘Final Notice: R. Raphaels & Sons Plc’ (29 May 2019) <https://www.fca.org.uk/publication/final-notices/r-raphael-sons-plc-final-notice-2019.pdf> accessed 4 August 2019

Financial Conduct Authority, ‘Final Notice: Royal Bank of Scotland Plc, National Westminster Bank Plc and Ulster Bank Ltd’ (19 November 2014) <https://www.fca.org.uk/publication/final-notices/rbs-natwest-ulster-final-notice.pdf> accessed 4 August 2019

Financial Conduct Authority, ‘Final Notice: Tesco Personal Finance Plc’ (1 October 2018) <https://www.fca.org.uk/publication/final-notices/tesco-personal-finance-plc-2018.pdf> accessed 4 August 2019

Financial Services Authority, ‘Final Notice: Zurich Insurance (UK) Plc’ (19 August 2010) <http://www.fsa.gov.uk/pubs/final/zurich_plc.pdf> accessed 21 June 2018

Financial Conduct Authority, ‘Good Cybersecurity - The Foundations’ (22 June 2017) <https://www.fca.org.uk/publication/documents/cyber-security-infographic.pdf> accessed 28 December 2020

Financial Conduct Authority, ‘Insights from the Cyber Coordination Groups’ (11 March 2020) <https://www.fca.org.uk/publications/research/insights-cyber-coordination-groups> accessed 20 December 2020

Financial Conduct Authority, 'Outsourcing in the life insurance sector' (4 March 2020) < https://www.fca.org.uk/publications/multi-firm-reviews/outsourcing-life-insurance-sector> accessed 4 August 2019

Financial Conduct Authority, 'Principles for Businesses' (August 2019) Schedule 2.2G <https://www.handbook.fca.org.uk/handbook/PRIN.pdf> accessed 4 August 2019

Financial Conduct Authority, 'PRIN2.1.1: The Principles' (3 January 2018) <https://www.handbook.fca.org.uk/handbook/PRIN/2/?view=chapter> accessed 21 June 2018

Financial Conduct Authority, 'Sector Views 2020' 13 <https://www.fca.org.uk/publication/corporate/sector-views-2020.pdf> accessed 28 December 2020

Financial Conduct Authority, SYSC 3 System and Controls <https://www.handbook.fca.org.uk/handbook/SYSC/3/1.html> accessed 28 December 2020

Financial Conduct Authority, 'The FCA's approach to advancing its objectives' (July 2013) 8 <https://www.fca.org.uk/publication/corporate/fca-approach-advancing-objectives-july-2013.pdf> accessed 4 August 2019

Financial Crimes Enforcement Network, 'Advisory to FIs on Cyber-Events and Cyber-Enabled Crime FIN-2016-A005' (25 October 2016) 7 <https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf> accessed 10 July 2020

Financial Services Authority, 'Final Notice: HSBC Life (UK) Limited' (17 July 2009) <http://www.fsa.gov.uk/pubs/final/hsbc_inuk0907.pdf> accessed 21 June 2018

Financial Services Information Sharing and Analysis Center, 'Exercises' <https://www.fsisac.com/hubfs/Resources/FS-ISAC_ExercisesOverview.pdf> accessed 10 July 2020

Financial Services Sector Coordinating Council, 'Financial Services Sector Specific Cybersecurity "Profile" *NIST Cybersecurity Workshop*' (17 May 2017) 11 <https://www.nist.gov/system/files/documents/2017/05/18/financial_services_csf.pdf> accessed 1 January 2021

Financial Stability Board, 'Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices' (13 October 2017) 7 <https://www.fsb.org/wp-content/uploads/P131017-1.pdf> accessed 14 July 2020

Financial Stability Oversight Council, '2019 Annual Report' (December 2019) 115 <https://home.treasury.gov/system/files/261/FSOC2019AnnualReport.pdf> accessed 12 July 2020

Financial Systemic Analysis and Resilience Center, 'US Treasuries (UST) Initiative Highlights Treasury Market Practices Group' (23 October 2018) 3 <https://www.newyorkfed.org/medialibrary/Microsites/tmpg/files/FSARC_TMPG_Presentation.pdf> accessed 23 July 2020

Financial Times, 'Virtual assets and financial crime now go hand in hand' (28 October 2018) <https://www.ft.com/content/8e26bba2-d91f-11e8-aa22-36538487e3d0> accessed 19 March 2021

First Bank of Nigeria Holdings (First Bank) Plc, '2019 Annual Report' 129 <https://www.fbnholdings.com/wp-content/uploads/2020/04/FBN_Holdings_Plc_2019_Annual_Report.pdf> accessed 16 September 2020

FRS, 'Information Technology Guidance' <https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm> accessed 18 August 2019

FRS, 'Interagency Guidance for response programs for unauthorised access to customer information and notice' (1 December 2005) 15 <https://www.federalreserve.gov/boarddocs/srletters/2005/SR0523.htm> accessed: 20 September 2019

FRS, 'Guidance on Managing Outsourcing Risk' (5 December 2013) 11 <https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf> accessed 15 July 2020

FSA Internal Audit Division, 'The supervision of Northern Rock: A Lessons Learned Review Report' (March 2008) para 26 <https://www.fca.org.uk/publication/corporate/fsa-nr-report.pdf> accessed 14 August 2019

FSB, 'Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices' (13 October 2017) 4 <http://www.fsb.org/wp-content/uploads/P131017-1.pdf> accessed 14 March 2019

FTC, 'Equifax to pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach' (*News Release,* 22 July 2019) <ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related> accessed 6 September 2019

Global Legal Group, 'The International Comparative Legal Guide to: Cybersecurity 2019' (October 2018) <https://www.acc.com/sites/default/files/resources/20190314/1492582_1.pdf> 17 November 2020

Guaranty Trust Bank (GT Bank) Plc, '2019 Annual Report' 25 <https://www.gtbank.com/uploads/financial-information/2019-Annual-Report.pdf> accessed 16 September 2020

HM Government, 'The UK Cyber Security Strategy - Protecting and promoting the UK in a digital world' 6 (November 2011) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> accessed 10 November 2020

HM Treasury, 'A new approach to financial regulation: building a stronger system' (February 2011) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/81411/consult_newfinancial_regulation170211.pdf> accessed 28 January 2021

HM Treasury, Financial Services Future Regulatory Framework Review Call For Evidence: Regulatory Coordination UK Finance Response (18 October 2019) paras 21 - 24 <https://ukfinance.org.uk/system/files/HMT%20call%20for%20evidence%20on%20regulatory%20coordinthation%20-%20UK%20Finance%20response.pdf> accessed 28 December 2020

House of Commons Committee of Public Accounts, 'The Growing Threat of Online Fraud: Sixth Report of Session 2017–19' (6 December 2017) 7 <https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/399/399.pdf> accessed 30 April 2018

IBM Security, '2018 Cost of a Data Breach Study: Global Overview' 5 <https://www.ibm.com/downloads/cas/861MNWN2> accessed 10 September 2019

IBM Security, 'Cost of a Data Breach Report 2019' 5 <https://www.ibm.com/downloads/cas/ZBZLY7KL> accessed 10 September 2019

Ibrahim A and others, 'A security review of local government using NIST CSF: a case study' (2018) 74 The Journal of Supercomputing 5171

IC3, '2016 Internet Crime Report' <https://pdf.ic3.gov/2016_IC3Report.pdf > accessed 6 September 2019.

IC3, '2017 Internet Crime Report' <https://pdf.ic3.gov/2017_IC3Report.pdf> accessed 6 September 2019.

IC3, '2018 Internet Crime Report' <https://pdf.ic3.gov/2018_IC3Report.pdf> accessed 6 September 2019

Internet Crime Complaint Center (IC3), '2019 Internet Crime Report' 3 <https://pdf.ic3.gov/2019_IC3Report.pdf> accessed 6 September 2019

Information Commissioner's Office, Credit reference agency Equifax fined for security breach (20 September 2018) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/credit-reference-agency-equifax-fined-for-security-breach/> accessed 28 December 2020

Information Commissioner's Office, 'Management Board' <https://ico.org.uk/about-the-ico/who-we-are/management-board/> accessed 19 January 2021

Information Commissioner's Office, NIS and the UK GDPR <https://ico.org.uk/for-organisations/the-guide-to-nis/nis-and-the-uk-gdpr/> accessed 6 January 2021

Institute of Directors, 'IoD Policy Report: Cyber security Ensuring business is ready for the 21st century (March 2017) <https://www.iod.com/Portals/0/PDFs/Campaigns%20and%20Reports/Digital%20and%20Technology/Cyber-Security-21stcentury.pdf?ver=2017-03-24-141846-840> accessed 8 July 2018

International Compliance Association, 'What is Financial Crime?' <https://www.int-comp.org/careers/a-career-in-financial-crime-prevention/what-is-financial-crime/> accessed 2 March 2021

International Monetary Fund, 'Financial System Abuse, Financial Crime and Money Laundering - Background Paper' (12 February 2001) <https://www.imf.org/external/np/ml/2001/eng/021201.pdf> accessed 5 March 2020

International Police Organization, Financial Crime. <https://www.interpol.int/Crime-areas/Financial-crime/Financial-crime> accessed 18 June 2017

International Telecommunication Union, 'Measuring digital development Facts and figures' (2019) 1 <https://www.itu.int/myitu/-/media/Publications/2020-Publications/Measuring-digital-development-2019.pdf> accessed 4 March 2021

Jake Rogers, 'Public-Private Partnerships: A Tool for Enhancing Cybersecurity' (2016) 19 <https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/40245/ROGERS-THESIS-2016.pdf?sequence=1&isAllowed=y> accessed 17 May 2021

Janina Hofer (2016) Report on risk perception: Deliverable D32.1 for Driver Project <https://driver-project.eu/wp-content/uploads/2017/11/Report-on-risk-perception.pdf> accessed 5 December 2019

JPMorgan Chase, 'Annual Report 2018' 35 <https://www.jpmorganchase.com/corporate/investor-relations/document/annualreport-2018.pdf> accessed 1 October 2019

Kaspersky, 'Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies' (3 April 2017) <https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies> accessed 10 November 2018

KPMG, ‘Cybersecurity: It’s Not Just about Technology’ (2014) <https://assets.kpmg.com/content/dam/kpmg/pdf/2014/05/cyber-security-not-just-technology.pdf> accessed 17 February 2017

Latham and Watkins LLP, ‘Cybersecurity regulation and best practice in the US and UK’ <https://www.lw.com/thoughtLeadership/Cybersecurity-regulation-and-best-practice> accessed 16 August 2018

Lawrence White, ‘British banks keep cyber attacks under wraps to protect image’ *Reuters* (London, 14 October 2016) < https://www.reuters.com/article/us-britain-banks-cyber/british-banks-keep-cyber-attacks-under-wraps-to-protect-image-idUKKBN12E0NQ?edition-redirect=uk> accessed 10 September 2019

Lending Standards Board, ‘Contingent Reimbursement Model Code for Authorised Push Payment Scams’ (28 May 2019) < https://www.lendingstandardsboard.org.uk/wp-content/uploads/2019/05/CRM-code.pdf> accessed 28 May 2020

LexisNexis, ‘Financial Services: Weekly highlights - 2 February 2017’<https://www.lexisnexis.co.uk/blog/financial-services/weekly-highlights-2-february-2017> accessed 10 June 2019

Lloyds Banking Group, ‘2018 Annual Report’ (19 February 2019) 74 <https://www.lloydsbankinggroup.com/globalassets/documents/investors/2018/2018_lbg_annual_report_v2.pdf> accessed 14 August 2019

Lloyds Banking Group, ‘2019 Annual Report’ 135 <https://www.lloydsbankinggroup.com/globalassets/documents/investors/2019/2019_lbg_annual_report_v3.pdf> accessed 6 June 2020

McAfee, ‘The Hidden Costs of Cybercrime’ (2020) 6 <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf> accessed 17 May 2021

Microsoft Tech Net, ‘Our commitment to our customers’ security’ (1 November 2016) <https://blogs.technet.microsoft.com/mmpc/2016/11/01/our-commitment-to-our-customers-security/> accessed 12 March 2021

National Audit Office, Online Fraud (30 June 2017) para 3.14 <https://www.nao.org.uk/wp-content/uploads/2017/06/Online-Fraud.pdf> accessed 13 August 2019

National Crime Agency, 'Public Private Threat Update Economic Crime - Key Judgements' (July 2019) <https://nationalcrimeagency.gov.uk/who-we-are/publications/323-public-private-threat-update-2019-economic-crime/file> accessed 2 August 2019

NDIC, '2018 Annual Report and Statement of Accounts' 113 <https://ndic.gov.ng/wp-content/uploads/2019/09/NDIC-2018-ANNUAL-REPORT.pdf> accessed 4 September 2020

NDIC, The Impact of Cybercrime on The Nigerian Economy and Banking System (March 2020) para 6.3 <https://ndic.gov.ng/wp-content/uploads/2020/03/NDIC-Quarterly-Q1-and-Q2-2019-Article-The-Impact-of-Cybercrime-on-The-Nigerian-Economy-and-Banking-System-.pdf> accessed 20 September 2020

NG-CERT, 'National Cyber Security Strategy' (December 2014) <https://www.cert.gov.ng/file/docs/NATIONAL_CYBESECURITY_STRATEGY.pdf> accessed 24 August 2018

Nigerian Deposit Insurance Corporation, '2019 Annual Report for the Year Ending December 31, 2019' para 13.2 <https://c5e9r5w9.rocketcdn.me/wp-content/uploads/2020/12/2019%20Annual%20Report%20Press.pdf> accessed 10 December 2020

Nigerian Computer Emergency Response Team, 'Advisories' <https://www.cert.gov.ng/advisories> accessed 19 September 2019

Nigeria Electronic Fraud Forum, 'A Changing Payments Ecosystem: The Security Challenge – Annual Report 2016' 33 <https://www.cbn.gov.ng/Out/2017/CCD/A%20CHANGING%20PAYMENTS%20ECOSYSTEM%20NeFF%202016%20Annual%20Report.pdf> accessed 9 November 2018

Nigerian Inter-Bank Settlement System, '2014 E-payment Fraud Landscape in Nigeria' 10 <http://www.nibss-plc.com.ng/wp-content/uploads/2015/03/Fraud-Landscape-2014.pdf> accessed 31 March 2019

NIST, 'Framework for Improving Critical Infrastructure Cybersecurity Version 1.1' 9 (16 April 2018) <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> accessed 12 October 2019

Norton Rose Fulbright LLP, 'Cybersecurity - not just an IT issue but a regulatory one too' (July 2017) <https://www.nortonrosefulbright.com/en/knowledge/publications/54263658/cybersecurity---not-just-an-it-issue-but-a-regulatory-one-too> accessed 10 February 2020

OAG, 'Citibank Complaint' <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/citibank_complaint.pdf?> accessed 14 July 2020

OCC, SEC, Cybersecurity and Resiliency Observations (27 January 2020) 2 <http://sec.gov/files/OCIE-Cybersecurity-and-Resiliency-Observations-2020-508.pdf> accessed 11 January 2021

OCC, 'OCC Hosts Compliance and Operational Risk Workshops in Los Angeles' (*News Release 103,* 9 September 2019) <https://www.occ.gov/news-issuances/news-releases/2019/nr-occ-2019-103.html> accessed 7 October 2019

OCC, 'Interagency White Paper on Sound Practices to Strengthen the Resilience of the US Financial System' (11 April 2003) 17813 <https://www.occ.treas.gov/news-issuances/bulletins/2003/OCC2003-14a.pdf> accessed 15 August 2019

OCC, OCC Bulletin 2013-29| Third-Party Relationships: Risk Management Guidance (30 October 2013) <https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html> accessed 8 October 2019

OCC, 'Semiannual Risk Perspective Spring 2019' 12 <https://www.occ.treas.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-spring-2019.pdf> accessed 8 October 2019

OCC, 'Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29' (5 March 2020) < https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html> accessed 15 July 2020

Office for National Statistics, ‘Crime in England and Wales: year ending Sept 2016’ (19 January 2017) <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016#whats-happening-to-trends-in-fraud> accessed 10 May 2018

Office of Compliance Inspections and Examinations, US Securities and Exchange Commission (SEC), ‘National Exam Program: Examination Priorities for 2016’ 3 <https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf> accessed 16 August 2018

Office of Financial Research, ‘Annual Report to Congress’ (2019) 39 <https://www.financialresearch.gov/annual-reports/files/OFR-Annual-Report-2019.pdf> accessed 15 July 2020

Office of the Attorney General, ‘Citibank Final Judgement’ <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/citibank_final_judgement.pdf?> accessed 14 July 2020

Office of the Comptroller of the Currency, ‘Fiscal Year 2020 Bank Supervision Operating Plan’ <https://www.occ.gov/news-issuances/news-releases/2019/2019-111a.pdf> accessed 7 October 2019

Payment Systems Regulator, ‘PSR kick-starts industry-wide effort to tackle payment scams’ (16 December 2016) <https://www.psr.org.uk/psr-publications/news-announcements/psr-kick-starts-industry-wide-effort-tackle-payment-scams> accessed 28 April 2018.

Peter Heyward, ‘Citigroup to Congress: Never Mind! (Some reflections on the Gramm-Leach-Bliley Act prompted by Citigroup's exit from insurance underwriting)’ (27 June 2005) 8 <https://www.venable.com/files/Publication/8d8da029-f4c3-4d37-9afa-2d9213dfc017/Presentation/PublicationAttachment/d6105a2e-bbd1-4c73-a265-8070f38d69d0/1335.pdf> accessed 21 July 2020

Ponemon Institute LLC, ‘Cyber Security on the Offense: A Study of IT Security Experts’ (November 2012) 1

<http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf > accessed 10 September 2019

PWC, 'Know Your Customer: Quick Reference Guide' (January 2014) <https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-anti-money-laundering-know-your-customer-quick-reference-guide.pdf> accessed 10 September 2019

Robert Eisenbeis, 'Can the President Fire the Chairman of the Federal Reserve?' (*Cumberland Advisors,* 10 January 2019) <https://www.cumber.com/can-the-president-fire-the-chairman-of-the-federal-reserve/> accessed 8 February 2021

RSA, 'White Paper: Strategies for Managing Ransomware Risk in Financial Services' (2020) 2 <https://www.rsa.com/content/dam/en/white-paper/strategies-for-managing-ransomware-risk-in-financial-services.pdf> accessed 19 May 2021

Sam Jones and Caroline Binham, 'Cyber security loophole found at bank' *Financial Times* (London, 3 March 2015) <https://www.ft.com/content/d71f8664-c103-11e4-88ca-00144feab7de> accessed 15 December 2017

SEC, 'CF Disclosure Guidance: Topic No. 2' (13 October 2011) <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm> accessed 16 August 2018

SEC, 'Commission Statement and Guidance on Public Company Cybersecurity Disclosures' (26 February 2018) 17 <https://www.sec.gov/rules/interp/2018/33-10459.pdf> accessed 10 November 2020

SEC, 'SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors' (25 September 2017) <https://www.sec.gov/news/press-release/2017-176 > accessed 16 September 2019

SEC, 'Statement on Cybersecurity' (20 September 2017) <https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20> accessed 12 September 2019

Serianu, Nigeria Cybersecurity Report 2017: Demystifying the Africa Cybersecurity Poverty Line' 11 (2017) <https://www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf> accessed 9 November 2018

S M Kerner, 'Why JPMorgan Chase Data Breach May Have Financial Fallout' (*eWeek*, 5 October 2014) <https://www.eweek.com/security/why-jpmorgan-chase-data-breach-may-have-financial-fallout> accessed 31 July 2020

Society for Risk Analysis, 'Risk Analysis Foundations' (7 May 2015) 4 <http://www.sra.org/sites/default/files/pdf/FoundationsMay7-2015-sent-x.pdf> accessed 3 December 2017

Surian Soosay, ''High risk' cyber-crime is really a mixed bag of threats' *The Conversation* (17 November 2014) <https://theconversation.com/high-risk-cyber-crime-is-really-a-mixed-bag-of-threats-34091> accessed 11 January 2022

TEISS, 'Banks to report all 'significant cyber incidents' to ECB starting this summer' (20 June 2017) <https://www.teiss.co.uk/banks-report-cyber-incidents-ecb-summer/> accessed 3 December 2017

The Chartered Institute of Bankers of Nigeria, 'Code of Conduct in The Nigerian Banking Industry 2013 (Professional Code Of Ethics And Business Conduct)' <https://www.cibng.org/files/resourceDownloads/codeOfConduct.pdf> accessed 1 April 2021

The National Fraud Center Inc, 'The Growing Global Threat of Economic and Cyber Crime' (December 2000) <http://www.utica.edu/academic/institutes/ecii/publications/media/global_threat_crime.pdf> accessed 10 March 2021

The Volcker Alliance, 'Reshaping the Financial Regulatory System: Long delayed, now crucial' (2015) <www.volckeralliance.org/sites/default/files/Reshaping%20the%20Financial%20Regulatory%20System%20-%20The%20Volcker%20Alliance.pdf> accessed 23 July 2020

TruSight, 'The New Industry Standard for Third-Party Risk Fact Sheet' <https://s3.us-east-1.amazonaws.com/trusightsolutions-com/documents/third-party-risk-assessment-fact-sheet-trusight-solutions.pdf?mtime=20190911161426> accessed 12 September 2019

UK Finance 'FRAUD THE FACTS 2018: The definitive overview of payment industry fraud' (31 July 2018) <https://www.ukfinance.org.uk/system/files/Fraud%20the%20facts-%20August%202018.pdf> accessed 28 May 2020

UK Finance 'FRAUD THE FACTS 2019: The definitive overview of payment industry fraud' 33 <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf> accessed 2 August 2019

UK Finance 'FRAUD THE FACTS 2020: The definitive overview of payment industry fraud' (14 May 2020) <https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-14-May.pdf> accessed 28 May 2020

United Nations Office on Drugs and Crime (UNODC), 'Comment on Good Practices, New Information on National Efforts and Recommendation with regards to the Meeting of the Open-Ended Intergovernmental Expert Group on Cybercrime (Submission from the Nigerian Financial Intelligence Unit (NFIU))' (March 2019) 3 <https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Comments/Nigeria_2.pdf> accessed 18 September 2020

United Nations, 'United Nations System Support for Capacity-Building E/2002/58' (14 May 2002) para 10 < https://digitallibrary.un.org/record/467223/files/E_2002_58-EN.pdf> accessed 10 May 2021

US Department of Justice, 'Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax' (10 Feb 2020) <www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking> accessed 23 July 2020

US DOJ, Deputy Attorney General Rod J Rosenstein Delivers Remarks at the Cambridge Cyber Summit Boston (4 October 2017) <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit> accessed 10 July 2020

US DOJ, 'Prosecuting Computer Crimes' 26 <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf> accessed 10 May 2021

US Government Accountability Office, 'Financial regulation: Complex and Fragmented Structure Could Be Streamlined to Improve Effectiveness' GAO-16-175 (25 February 2016) 2 <https://www.gao.gov/assets/680/675400.pdf>

US GAO, ‘Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach’ (August 2018) 7 <https://www.gao.gov/assets/700/694158.pdfa> accessed 14 July 2020

US Senate, ‘How Equifax Neglected Cybersecurity and Suffered A Devastating Data Breach: Staff Report Permanent Subcommittee on Investigations’ <www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf > accessed 15 July 2020

United States Congress, ‘H.R.5069 - Cybersecurity Systems and Risks Reporting Act’ <https://www.congress.gov/bill/114th-congress/house-bill/5069/text> accessed 11 October 2019

White House, ‘Cyber Security Funding’ 305 <https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf> accessed 10 November 2020

World Bank Group, ‘Financial Sector Advisory Center - Financial Sector’s Cybersecurity: A Regulatory Digest’ (July 2020) <https://pubdocs.worldbank.org/en/361881595872293851/CybersecDigest-v5-Jul2020-FINAL.pdf> accessed 10 September 2020