Cyber-Risks in Modern Finance:
Building Operational and Regulatory Resilience

Dr. Jonathan McCarthy *

Introduction

The COVID-19 pandemic has arguably contributed more than any other contemporary development to an increase in public awareness of technological systems' vulnerabilities to cyber-attacks. The risks to financial services inevitably generate acute unease among institutions, businesses, and, in particular, customers who stand to lose most when there are threats to accounts, privacy, and personal data. The incremental digitalisation of modern finance places an onus squarely on financial institutions and firms to adapt their defences to cyber-risks. In parallel with institutional efforts to protect the operational resilience of information technology (IT) systems, existing regulatory frameworks are expected to appropriately adapt and become resilient to the emergence of new cyber-risks.

Operational resilience is inextricably intertwined with the strength of regulation. If regulation is unable to tell how cyber-risks are changing, then how effective will regulation be in tackling the problems which result from successful cyber-attacks and other incidents?

This article commences by pinpointing the distinct patterns in cybersecurity threats which are being revealed since the pandemic, specifically in relation to finance. In view of the changing nature of cyber-risks, the article emphasises how standards for system resilience need to be clear, but flexible. Gradual progress is being made by international agencies – such as the Financial Stability Board (FSB), the International Organization of Securities Commissions (IOSCO), the European Systemic Risk Board (ESRB), and the G7 – towards devising coherent standards to apply to various aspects of cybersecurity. The recent pre-eminent instance of the creation of a regime to mitigate cyber-risks in finance is the European Union's Digital Operational Resilience Act (DORA), as enacted by Regulation (EU) 2022/2554. [1] DORA

* Lecturer, School of Law, University College Cork, Ireland. Email: Jonathan.McCarthy@ucc.ie

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ L 333/1 [hereinafter 'DORA'].

imposes requirements on financial entities to, *inter alia*, strengthen systems, recognise likely threats, report the occurrence of incidents, and comply with mandatory provisions in contractual arrangements with third party service providers.

Although the article will explain how regulatory measures must be implemented by EU supervisory authorities following DORA's entry into force, standards of testing and reporting of cyber-risks can still vary from institution to institution. The article will analyse the difficulties involved in establishing precise testing and reporting standards across financial services. These difficulties exacerbate the problems in attempting to coordinate standards for convergence generally between international cybersecurity frameworks. The article will acknowledge that legislation may only be able to travel some of the distance to robustly guard against cyber-risks in finance. Sector-led standards – including institutional governance procedures and codes of conduct – will continue to be decisive in reducing the prospect of widespread systemic collapses.

Cybersecurity threats since the COVID-19 pandemic

During a pandemic era of remote working and a manifestly growing reliance on digital technologies, it would be unsurprising to find that concerns about cybersecurity became more prevalent among financial professionals and practitioners. The concerns are underscored by evidence that cyber-attacks are now markedly more frequent and more severe than the figures reported over the past decade. [2] As presented through European Central Bank (ECB) research, the calculated overall amount of publicly disclosed cyber-attacks has accordingly increased public awareness (as exemplified by Internet searches for terms relating to cyber-attacks) of cybersecurity and increased the revenue directed towards preventing cybercrime. [3] Disclosed cyber-attacks appear to have reached a peak during 2020 (in the midst of the most stringent of COVID-19 restrictions internationally), as the health care and public administration sectors were subjected to a higher proportion of criminally motivated, or malicious, cyber-attacks than the finance and insurance sector of the global economy. [4] However, as expressed in other studies, a lower degree of cyber-attacks in finance does not infer that finance is simply not

[2] J. Fell, N. de Vette, S. Gardó, B. Klaus, and J. Wendelborn, 'Towards a Framework for Assessing Systemic Cyber Risk' in ECB, *Financial Stability Review* (November 2022).
[3] Fell et al, 'Towards a Framework for Assessing Systemic Cyber Risk', Chart C.1, p. 118.
[4] Fell et al, 'Towards a Framework for Assessing Systemic Cyber Risk', Chart C.4, p. 122.

exposed to the same level of risk, but rather that current protections against cyber-attacks are functioning strongly and that risks are more effectively managed. [5]

The cyber-risks which are materialising at present are essentially a continuation of patterns from previous years. Ransomware and malware, threats against personal data (leading to extortion claims against victims of cyber-attacks), and geopolitical tensions (particularly in the context of the war between Russia and Ukraine and 'hacktivism' on grounds of political/ethical protest) are discerned as being primary catalysts for the development of cyber-risks. [6] An escalating 'arms race' between cyber-attackers and cybersecurity professionals, a fragmentation of regulatory frameworks, insufficient internal governance standards, and lack of investment in resources and skills could equally be added as pivotal factors. [7]

Ransomware and other forms of malware are consistently identified as key threats to organisational IT systems and to businesses. [8] As defined by the FSB's updated 'Cyber Lexicon', 'malware' is "[s]oftware designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems." [9] The FSB definition of 'ransomware' is malware "that is used to commit extortion by impairing the use of an information system or its information until a ransom demand is satisfied." [10] The indications are that ransomware, as commonly used with phishing messages, represents the major threat to organisations and firms in the public and private sectors. [11] In return for restoring access to decrypted data, ransoms may often be made payable to attackers through cryptocurrencies, although there are suggestions that victims are no longer as prepared to accede to ransomware demands. [12] As affirmed by ECB research findings, crypto-assets

---

[5] I. Aldasoro, L. Gambacorta, P. Giudici, and T. Leach, 'The Drivers of Cyber Risk' (BIS Working Paper No. 865) (May 2020), p. 19.
[6] See generally ENISA, *ENISA Threat Landscape (July 2021 to July 2022)* (October 2022).
[7] See Bipartisan Policy Center, *Top Risks in Cybersecurity 2023* (Washington D.C., 2023).
[8] For instance, see Accenture, *Threats Unmasked: 2021 Cyber Threat Intelligence Report* (Volumes 1 and 2); available at: https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence-report-2021 (date accessed: 27 April 2023).
[9] FSB, *Cyber Lexicon* (2023 Update), p. 12; available at: https://www.fsb.org/2023/04/cyber-lexicon-updated-in-2023/ (date accessed: 27 April 2023).
[10] FSB, *Cyber Lexicon* (2023 Update), p. 13.
[11] For a summary of emerging details regarding current cyber-threats, see C. Brooks, 'Cybersecurity Trends and Statistics For 2023; What You Need To Know' (Forbes, 5 March 2023); available at: https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=737541819dba (date accessed: 27 April 2023).
[12] Chainalysis, *The 2023 Crypto Crime Report* (February 2023); available at: https://go.chainalysis.com/2023-crypto-crime-report.html (date accessed: 27 April 2023).

remain the dominant method of payment in response to cyber-attacks. [13] Moreover, other research findings have revealed a positive correlation between the value of the Bitcoin cryptocurrency and the intensity of cyber events involving cryptocurrencies. [14] Yet, ransomware may not always have to be deployed by attackers. For example, 'cryptojacking' attacks can, in effect, surreptitiously use operational systems and devices to mine cryptocurrencies without victims' knowledge. [15]

In light of a proliferation of potential cyber-risks, it could be argued that the responsibility is ultimately on financial institutions and firms to strive to protect their own systems and customers. Two limitations to this argument are that cybersecurity insurance is not extensively used by firms and that there are intricate interdependencies with third party service providers, notably with a concentrated number of providers of cloud computing services for data storage. Cybersecurity insurance premiums are steadily increasing [16] and the value of the cybersecurity insurance market globally is expanding. [17] However, as demonstrated by European Union Agency for Cybersecurity (ENISA) survey findings, a significant majority of EU organisations do not have cybersecurity insurance. [18] For certain respondents to the ENISA survey, alternative measures (such as investing further in Chief Information Security Officers, or equivalent positions, within organisations) were deemed to be more appropriate than accepting the costs and relatively restricted coverage of a cybersecurity insurance policy. [19] Institutional use of similar cloud services can produce a 'cyber-monoculture' [20], whereby various market players are exposed to interconnected risks from a narrow range of cloud providers. The interactions between cloud vendors and a series of institutional or business clients can augment cybersecurity challenges and can increase exposures to cyber-threats. [21] Within an outsourcing setting, a successful attack on a cloud provider's system could consequently compromise the systems of multiple clients across the financial services sector.

---

[13] Fell et al, 'Towards a Framework for Assessing Systemic Cyber Risk', p. 124.
[14] Aldasoro et al, The Drivers of Cyber Risk' (BIS Working Paper No. 865) (2020).
[15] See Accenture, *Threats Unmasked: 2021 Cyber Threat Intelligence Report* (Volume 2).
[16] Fell et al, 'Towards a Framework for Assessing Systemic Cyber Risk', Chart C.7, p. 126.
[17] See Fortune Business Insights, Cyber Insurance Market, available at: https://www.fortunebusinessinsights.com/cyber-insurance-market-106287 (date accessed: 27 April 2023).
[18] ENISA, *Demand Side of Cyber Insurance in the EU* (ENISA, February 2023).
[19] ENISA, *Demand Side of Cyber Insurance in the EU* (2023), p. 15.
[20] R. Buckley, D. Arner, D. Zetzsche, and E. Selga, 'TechRisk' (2020) 3 *Singapore Journal of Legal Studies* 35.
[21] See especially ENISA, *Cloud Cybersecurity Market Analysis* (ENISA, March 2023), 2.4 and 2.5, pp. 22–24.

As the international cloud services market is mastered by the familiar lynchpins of Amazon, Microsoft and Google, the repercussions of a costly cyber-attack and system failure would signify that cloud computing should be treated as a systemically important infrastructure. [22] However, it is regularly questioned whether cyber-risks could be interpreted as being truly systemic risks within the financial sector, particularly depending on how systemic risk itself is understood. [23] As a reasonable proposition, a cyber-attack is capable of drastically impeding and harming a financial system's normal functions and activities. Customers will be adversely impacted, and, in turn, there can be detrimental effects on the wider economy. ESRB research has elaborated on how cyber-risks can have shock and amplification outcomes, culminating in a disruptive systemic event (a 'crash') which impairs all or part of the financial system and which potentially has negative serious consequences for the real economy. [24] Critical disruption of this kind can conceivably transpire from a plethora of cyber-risks – be it from ransomware, malware, phishing, denial of service attacks, concealed mining, theft of funds or data – and can transpire on a global scale.

International standard-setting

When discussing the risks affecting IT systems and operational resilience across finance globally, it is beneficial to have an internationally recognised and clear definition as to what is meant by cyber-risks and related terms. Albeit an obvious starting point for any analysis of cyber-risks in finance, attaining consensus on the relevant terminology is also crucial to subsequently constructing international standards for collaboration and coordination.

As alluded to above, the FSB's updated Cyber Lexicon constitutes the most prominent example of establishing definitions, or a 'common understanding' [25], for the purposes of cybersecurity in finance. To focus on some of the terms which are most central to this article, a 'cyber risk' in the FSB Cyber Lexicon denotes "[t]he combination of the probability of cyber incidents occurring and their impact." [26] A 'cyber incident' is a "cyber event that adversely affects the

[22] R. Macrae and J. Danielsson, 'Systemic Consequences of Outsourcing to the Cloud' (VoxEU column, 2 December 2019); available at: https://cepr.org/voxeu/columns/systemic-consequences-outsourcing-cloud (date accessed: 27 April 2023).
[23] M. Fouche, R. Macrae and J. Danielsson, 'Cyber Risk as Systemic Risk' (VoxEU column, 10 June 2016); available at: https://cepr.org/voxeu/columns/cyber-risk-systemic-risk (date accessed: 27 April 2023).
[24] G. Ros, 'The Making of a Cyber Crash: A Conceptual Model for Systemic Risk in the Financial Sector' (ESRB Occasional Paper No. 16) (May 2020).
[25] FSB, *Cyber Lexicon* (2023 Update), pp. 5–6.
[26] FSB, *Cyber Lexicon* (2023 Update), p. 10.

cyber security of an information system or the information the system processes, stores or transmits whether resulting from malicious activity or not." [27] As a comparably benign scenario, a 'cyber event' is "[a]ny observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring." [28] As the deliberately harmful scenario, a 'cyber attack' is "[m]alicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt or gain unauthorized access to assets." [29]

The FSB categorisation of terminology is designed to support the standard-setting of other international agencies and the Cyber Lexicon is continually being referred to in institutional reports and publications. [30] Beyond the publication and updating of its Cyber Lexicon, the FSB has been integral to progressing international standard-setting in respect of several facets of cybersecurity in finance. At the time of writing, two of the foremost FSB publications are the final report on achieving greater convergence in cyber incident reporting (containing a total of sixteen recommendations) [31] and a proposal for a Format for Incident Reporting Exchange (FIRE). [32]

From the perspective of central banking authorities, it is vital that cohesive standards, recommendations, and guidelines can be referred to, and seamlessly implemented, within domestic regulatory frameworks. The Basel Committee on Banking Supervision (BCBS)'s Principles for Operational Resilience, as released in March 2021, [33] acknowledged the influence of the COVID-19 pandemic in formulating feasible governance standards to absorb, and cope with, unforeseen disruptions. Aside from global pandemics and natural disasters, the principles-based approach conveyed by the 2021 Principles is intended be appropriate in responding to a range of possible shocks to the resilience of the financial system, including cyber incidents and risks to cybersecurity. The maintenance of business continuity and critical operations is a fundamental objective of internal planning, detection, testing, and recovery

[27] FSB, *Cyber Lexicon* (2023 Update), p. 10.
[28] FSB, *Cyber Lexicon* (2023 Update), p. 10.
[29] FSB, *Cyber Lexicon* (2023 Update), p. 10.
[30] Even though the Cyber Lexicon is a comprehensive glossary of terms for international bodies, it is noted in the FSB document that "[t]he terms and definitions in the lexicon were developed only for use with respect to the financial services sector and the financial institutions therein. The lexicon is not intended for use in the legal interpretation of any international arrangement or agreement or any private contract."
[31] FSB, *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting. Final Report* (April 2023).
[32] FSB, *Format for an Incident Reporting Exchange (FIRE). A Possible Way Forward* (April 2023).
[33] BCBS, *Principles for Operational Resilience* (BIS, March 2021).

measures. [34] The emphasis on central banks' adoption of cyber-risk mitigation measures is reflected in Bank for International Settlements (BIS) research findings showing that over 80% of the respondents from central banking authorities in advanced economies are conducting simulation exercises (or 'fire drills') at least once a year. [35]

In October 2017, a Cyber Task Force was launched by IOSCO, and its final report in 2019 completed a review of three Core Standards for cybersecurity. [36] Firstly, the National Institute of Standards and Technology (NIST) cybersecurity framework is a voluntary, US-based framework for operators of critical infrastructure. Secondly, as a framework which is international in scope, the Committee on Payments and Market Infrastructures (CPMI) – IOSCO framework provides guidance on cyber resilience for financial market infrastructures (FMIs). The guidance revolves around five 'primary risk management categories' (governance; identification; protection; detection; and response and recovery) which are complemented by three 'overarching components' of testing, situational awareness, and evolving and learning. [37] Thirdly, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) frameworks are used generally by multinational corporations and can incur charges when updating systems to comply with these frameworks.

Consistency in international cybersecurity standards for finance is also moulded by G7 reports which expand on the G7's 'Fundamental Elements of Cybersecurity for the Financial Sector' from 2016. [38] There are eight elements set out in the original G7 document which are designed for entitles in the financial sector: establishing and maintaining a cybersecurity strategy and framework; defining and facilitating governance; identifying risk and control assessment; establishing systematic monitoring processes; implementing timely incident response policies and other controls; allowing for prompt and effective recovery of operations; engaging in timely sharing of information; and reviewing cybersecurity strategies and frameworks regularly as a continuous learning process.

---

[34] See especially Principle 3 of BCBS, Principles for Operational Resilience (BIS, March 2021), pp. 5–6.
[35] S. Doerr, L. Gambacorta, T. Leach, B. Legros, and D. Whyte, 'Cyber Risk in Central Banking' (BIS Working Paper No. 1039) (September 2022), Graph 3, p. 10. According to the same data, over 70% of supervisors from emerging market economies are completing cyber-exercises at least once a year.
[36] IOSCO, *Cyber Task Force – Final Report* (FR09, June 2019).
[37] As an example of a review of these principles in application, see CPMI-IOSCO, 'Implementation monitoring of the PFMI: Level 3 assessment on Financial Market Infrastructures' Cyber Resilience' (November 2022).
[38] See the European Commission website at: https://finance.ec.europa.eu/publications/g7-fundamental-elements-cybersecurity-financial-sector_en (date accessed: 27 April 2023).

In October 2022, the G7 issued separate documents revisiting the above fundamental principles in relation to ransomware resilience in the financial sector and to third party cyber risk management. [39] In reinforcing a response to cyber-risks which was noted in the preceding section of this article, the fundamental principles on ransomware resilience stipulate how "G7 countries generally discourage ransom payments", so as to deter against ongoing criminality and continued malicious attacks. This stance is recommended in circumstances when there is little guarantee that victims' access to data will be restored or that attackers will not retain copies of sensitive data. [40]

Standard-setting efforts are evident at a jurisdictional level within the UK, the US, and – as a particular focus of the next section of the article – the EU. In 2021, the Bank of England and the UK's Financial Conduct Authority committed to a 'Transforming Data Collection' programme to adopt and refine common data and reporting standards. [41] In 2022, the Cyber Incident Reporting for Critical Infrastructure Act was signed into US law. The legislation requires the Cybersecurity and Infrastructure Security Agency (CISA) to implement reporting requirements by obliging eligible entities to disclose cyber-attacks such as ransomware. [42]

A corresponding move towards standardised incident reporting is being advocated by EU authorities such as the ESRB and the ECB. Proposals on incident reporting measures will be further assessed in the final section of the article. The EU's espousal of foundational policies to support cybersecurity and operational resilience is matched by a growing fabric of legislative measures, namely the 'Cybersecurity Act' of 2019 [43], the second Network and Information Systems Directive of 2022 [44], and the European Commission's proposal for a 'Cyber Resilience

[39] G7, 'Fundamental Elements for Ransomware Resilience for the Financial Sector' (October 2022) and 'Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector' (October 2022).
[40] G7, 'Fundamental Elements for Ransomware Resilience for the Financial Sector' (2022), p. 2 (Element 2: Governance)
[41] See the Bank of England website at: https://www.bankofengland.co.uk/prudential-regulation/transforming-data-collection (date accessed: 27 April 2023) and the FCA's website at: https://www.fca.org.uk/firms/transforming-data-collection (date accessed: 27 April 2023).
[42] See the CISA website at: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia (date accessed: 27 April 2023).
[43] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, OJ L 151.
[44] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, OJ L 333.

Act' pertaining to products with digital elements. [45] However, as this article is focused on the measures being taken to diminish cyber-risks in finance, the article must provide an overview of the landmark EU legislative initiative specific to financial entities, the DORA Regulation, as enacted in 2022.

The EU example: Digital Operational Resilience Act

As introduced by Regulation (EU) 2022/2554, DORA is the most resolute signal of the EU's intent to apply harmonised standards for operational resilience in the financial sector. Although the Regulation will fully apply as from 17 January 2025 [46], DORA bolsters the original policy goals of the European Commission's Digital Finance Strategy (as published in 2020) in promoting certainty about the EU's future regulatory approach with regard to evolving aspects of digitalisation and technological innovation in finance. [47] From the vantage of other jurisdictions, DORA serves as an instructive test of how practicable it should be to enforce uniform requirements and obligations for operational resilience in finance.

In light of this article's appraisal of 'resilience' in terms of system operations and regulation, perhaps the most logical beginning to a summary of DORA's provisions is to consider the definition which the Regulation places on 'digital operational resilience'. 'Digital operational resilience' connotes "the ability of a financial entity to build, assure and review its operational integrity and reliability" and, in so doing, "by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses…" These are systems which "support the continued provision of financial services and their quality, including throughout disruptions." [48]

The eligible 'financial entities' encompassed within DORA's scope, include credit and payment institutions, electronic money institutions, investment firms, crypto-asset service

[45] European Commission, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final.
[46] DORA, Article 64.
[47] The author's analysis of the initial Commission proposal for a DORA Regulation, within the broader Digital Finance Strategy, is available in this Journal as: J. McCarthy, 'Evaluating the EU's Digital Finance Strategy: Ambitious Glimpses of Future Regulation?' (2021) 36(9) *Journal of International Banking Law and Regulation* 379.
[48] DORA, Article 3(1).

providers, central securities depositories (CSDs), central counterparties, trading venues, managers of alternative investment funds (AIFs), insurance and reinsurance undertakings and intermediaries, credit agencies, crowdfunding service providers, and ICT third-party service providers. [49]

Chapter II of DORA's provisions – from Articles 5 to 16 – is based on ICT risk management. Financial entities are required to have in place internal governance and control frameworks to ensure "prudent and effective" management of ICT risk. [50] The responsibility for maintaining the frameworks rests with financial entities' management bodies. [51] Obligations are on financial entities to use and maintain updated ICT systems, protocols, and tools. [52] Entities are required to continuously engage in identification of possible sources of ICT risk and, at least on an annual basis, entities should review risk scenarios which impact on those entities. [53] Entities must adequately deploy protection and prevention measures [54] and "have in place mechanisms to promptly detect anomalous activities" (including network performance issues, incidents, and potential material single points of failure). [55] As response and recovery measures, entities must have comprehensive business continuity policies [56], as accompanied by developed and documented 'backup policies and procedures, and restoration and recovery procedures and methods.' [57] Information-gathering capabilities and staff are mandatory for financial entities [58] and entities must have crisis communication plans for responsible disclosure of major ICT incidents or vulnerabilities, where appropriate. [59] The European Supervisory Authorities (ESAs), in conjunction with ENISA, will draft common regulatory technical standards on risk

[49] DORA, Article 2(1).
[50] DORA, Article 5(1).
[51] DORA, Article 5(2).
[52] DORA, Article 7.
[53] DORA, Article 8(2). By Article 8(3), financial entities, other than microenterprises, must perform risk assessments upon major changes to network and information system infrastructures, while, under Article 8(6), maintaining relevant inventories which must be updated periodically and after every major change to infrastructures. A microenterprise is defined in Article 3(60) as a financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed €2 million.
[54] DORA, Article 9.
[55] DORA, Article 10.
[56] DORA, Article 11.
[57] DORA, Article 12. By Article 12(5), CSDs are to maintain at least one secondary processing site in the interests of continuity of critical or important functions of the primary site.
[58] DORA, Article 13.
[59] DORA, Article 14.

management frameworks and ICT policies, which are to be submitted to the European Commission by 17 January 2024. [60]

Chapter III of the provisions – from Articles 17 to 23 – are centred on ICT incident reporting. Financial entities must "define, establish, and implement" incident management processes to detect, manage and notify incidents. [61] These processes should entail early warning indicators, procedures for identification, tracking and logging of incidents according to priority and severity and the criticality of services impacted, and plans for communication to staff, external stakeholders, and media. [62] ICT-related incidents and cyber threats are to be classified by financial entities by criteria stated in the Regulation, [63] but which will be further specified by ESA draft regulatory technical standards to be submitted to the European Commission by 17 January 2024.

Major ICT-related incidents must be reported by financial entities to relevant competent authorities. [64] Voluntary notifications are permissible if a threat is deemed "to be of relevance to the financial system, service users or clients." [65] DORA provides that "[w]here a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, inform their clients" about the incident itself and about the measures being taken "to mitigate the adverse effects of such incident." [66] The harmonisation of reporting content, templates and time limits for initial notification is to be achieved through common regulatory technical standards, a draft of which must be submitted by the ESAs to the Commission by 17 July 2024. [67]

The legislation envisages that financial entities' incident reporting could be centralised through a single EU Hub "with a view to enhancing supervisory convergence." [68] Having consulted

[60] DORA, Article 15.
[61] DORA, Article 17.
[62] DORA, Article 17(3).
[63] DORA, Article 18. The impact of incidents may be determined by such criteria as: the number and/or relevance of clients or financial counterparts affected, and, where applicable, the amount or number of transactions affected, and whether reputational damage was caused; the duration of the incident (including service down-time); the geographical spread; data losses; the criticality of the services affected; and the economic impact. Cyber threats should be classified as 'significant' "based on the criticality of the services at risk", which includes transactions and operations, clients or financial counterparts, and geographical spread.
[64] DORA, Article 19(1).
[65] DORA, Article 19(2).
[66] DORA, Article 19(3).
[67] DORA, Article 20.
[68] DORA, Article 21(1).

with the ECB and ENISA, an ESAs Joint Report on the feasibility of a centralised structure for incident reporting must be submitted to the European Parliament, the Council of the European Union, and the Commission by 17 January 2025. [69]

Chapter IV of the provisions – from Articles 24 to 27 – pertain to testing. Appropriate tests of ICT tools and systems are specified as: vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing. [70] The fact that the provisions explicitly classify certain tests as being more suitable creates a hurdle for the legislation in proving its ability to adapt to future changes in testing techniques. Yet, the legislation goes a step further by making threat-led penetration testing a fulcrum of the advanced testing which is envisioned by the provisions.

With exceptions for some categories [71], financial entities must carry out threat-led penetration advanced testing at least every three years, although competent authorities may request the frequency of this testing to be reduced or increased. [72] The object of each threat-led penetration test is to "cover several or all critical or important functions of a financial entity" and must be "performed on live production systems supporting such functions." [73] Joint draft regulatory technical standards are to be developed by the ESAs, in agreement with the ECB, and are to be submitted to the Commission by 17 July 2024. [74] These standards are to be drafted in accordance with the present TIBER-EU framework of testing, which will be referred to in the next section of the article.

Chapter V of DORA's provisions – from Articles 28 to 44 – is on management of third-party risk. This element of the legislation is evidently intrinsic to mitigating cyber-risks, as indicated above when evaluating the risks associated with cloud providers. However, the most

[69] DORA, Article 21(3).
[70] DORA, Article 25(1).
[71] Aside from microenterprises (see the definition in n. 53 above), DORA's Article 16 provides for exclusions for small and non-interconnected investment firms, payment institutions and e-money institutions who are exempt pursuant to the Payment Services Directive (Directive (EU) 2015/2366) and the e-Money Directive (Directive 2009/110/EC), institutions exempted pursuant to the Credit Institutions Directive (Directive 2013/36/EU) where EU Member States have not exercised the option to remove such institutions from the exemption, and small institutions for occupational retirement provision.
[72] DORA, Article 26(1).
[73] DORA, Article 26(2).
[74] DORA, Article 26(11).

substantive aspects of DORA for this article's focus are tied to testing and reporting requirements. In terms of third-party risks, financial entities are required to execute an assessment of 'concentration risk' arising from a contractual arrangement with a third-party service provider. [75] Key contractual provisions are obligated for arrangements on the use of ICT services. [76]

Information-sharing arrangements are enabled through Chapter VI of DORA. The exchange of cyber-threat information and intelligence between financial entities – thus allowing for notifications to competent authorities – is facilitated by the legislation. [77] However, in practice, the growth of collaborative platforms will be a work-in-progress. As argued in the next section, the mechanisms for testing and reporting are a prime area by which knowledge can be exchanged, not only to guarantee compliance with legislative obligations, but also to assist in establishing coordinated sectoral standards.

Clarifying testing and reporting standards

Even though the EU's DORA is an immense initiative by any measure of a legislative effort to regulate for cyber-risks in finance, it is but part of the progress towards international standards for testing of cyber-risks and for reporting of cyber incidents and cyber-attacks. The aspirations in standard-setting can be plain to see. Yet, it can be more difficult to precisely delineate what coordinated testing and reporting frameworks should look like and how these frameworks are to function.

An unavoidable preliminary aim must be to confront institutional weaknesses and hesitancy in engaging in effective testing and reporting. As ascertained by the FSB's 2023 final report on achieving greater convergence in cyber incident reporting, a culture of late reporting of incidents can profoundly hamper financial institutions' responses to widespread incidents which can escalate to crises. [78] The origins of the problem are typically rooted in early assessment challenges, as characterised by a lack of information at early stages of incidents

[75] DORA, Article 29. Furthermore, Article 31 provides for the designation of critical ICT third-party service providers who will be made subject to an oversight framework.
[76] DORA, Article 30.
[77] DORA, Article 45
[78] FSB, *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting. Final Report* (April 2023)

and/or receiving information from third-party service providers regarding incidents. There are several possible 'causal factors' for the impediments to timely reporting, including organisational culture or lack of awareness of the consequences of cyber-risks, inadequate decision-making capabilities and reporting procedures, an absence of clear regulatory requirements, and fear of reputational damage or lack of trust within an institution. [79]

Notwithstanding the significance which DORA ascribes to techniques of threat-led penetration testing, financial institutions should be cognisant of how best to implement practical and graduated methods that can be tailored to the organisational needs of a given institution. For instance, simulation exercises, scenario testing, and 'war games' are means by which existing ICT systems are not only tested but are also expected to absorb some manageable risk or threat. In a European context, the ESRB has advocated for system-wide piloting of measures of cyber-resilience scenario testing (CyRST) as an analytical tool. [80] According to the ESRB, magnified cyber-threats to Ukraine and EU Member States in the wake of Russia's invasion of Ukraine have elevated the necessity for such a systemic approach to testing. The distinctive feature of scenario testing is that, unlike any rudimentary testing technique, "it could enable an assessment of how the financial system would respond to and recover from a severe but plausible cyber scenario." [81] Depending on the size of a financial institution and the scale of its activities, the expertise and resources put towards scenario testing can be adjusted, particularly to guarantee that the recovery after the initial testing is kept manageable.

It would be an incomplete framework if responsibility were to be confined exclusively to financial institutions. When conducting assessments of cyber-risks, supervisory authorities should acquire an overall picture of the potential latent vulnerabilities to operational resilience. As a complementary analytical tool with scenario testing, the ESRB proposition is for authorities to set 'systemic impact tolerance objectives' (SITOs), which "define the point at which the tolerance of disruption of the financial system is deemed to be breached and are distinct from the impact tolerance levels of individual institutions." [82] By recognising that the delivery of key economic functions can eventually be radically disrupted by cyber incidents, a SITO is as close an acknowledgement as possible of how cyber-risks can amount to fully-

[79] See especially Figure 3, p. 9, of FSB, *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting. Final Report* (2023).
[80] ESRB, *Advancing Macroprudential Tools for Cyber Resilience* (February 2023).
[81] ESRB, *Advancing Macroprudential Tools for Cyber Resilience* (2023), p. 10.
[82] ESRB, *Advancing Macroprudential Tools for Cyber Resilience* (2023), p. 21.

fledged systemic risks. When applying this testing model to the wider financial system, 'intervention ladders' could be utilised to enhance subsequent reporting. [83] After a cyber 'shock' triggers a pre-determined alert threshold, any amplification will cause authorities to deploy reaction measures. Any further escalation may hit the SITO impact level and become a legitimately systemic event.

Coordinated frameworks of scenario testing by financial institutions, complemented by the SITOs as defined by supervisory authorities, must be built on foundations of collaborative information-sharing networks. An exemplary reference-point is the EU's Cyber Information and Intelligence Sharing Initiative (CIISI–EU). The CIISI–EU was established in September 2020 by members of the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB). [84] Moreover, the ECRB itself is proactive in working to safeguard systemic stability during an unprecedented period of risks linked to emergent technologies, such as crypto-assets and artificial intelligence. [85] The CIISI–EU allows for collaborative platforms and meetings between public and private sector entities to share knowledge on tackling cyber-risks. As protocols for the CIISI–EU's intelligence-sharing work, there are three categories of information to be exchanged. [86] Strategic information is contributing to decision-making and planning in the mid– to long-term. Operational information is shaped by analyses of the capabilities and methodologies of cyber-attacks. Tactical information is preoccupied with the exact tools and methods of cyber-attacks or hacking of systems. As an EU example, the CIISI–EU network epitomises how testing and reporting frameworks can flourish from two innate ingredients: collaborative sharing of information between financial institutions and supervisory authorities; and clarity as to the categories of information to be exchanged. [87]

---

[83] ESRB, *Advancing Macroprudential Tools for Cyber Resilience* (2023), section 3.3, pp. 25 – 26.

[84] See the report on the ECB website at: https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews200915.en.html (date accessed: 27 April 2023).

[85] See speech of Fabio Panetta, Member of the ECB Executive Board, at the ECRB meeting in Frankfurt am Main, 8 March 2023, 'The Quick and the Dead: Building Up Cyber Resilience in the Financial Sector'; available at: https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230308~92211cd1f5.en.html (date accessed: 27 April 2023).

[86] ECB – Euro Cyber Resilience Board Secretariat, *Cyber Information and Intelligence Sharing Initiative (CIISI-EU. Cyber Information and Intelligence Sharing: A Practical Example* (September 2020), 7. Protocols for Sharing Intelligence; available at: https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ciisi-eu_practical_example.pdf (date accessed: 27 April 2023).

[87] In adhering to a similar structure for coordinated standards, the ESRB has issued a recommendation for a new pan-European systemic cyber incident coordination framework which will accompany the entry into force of DORA. Once the EU-SCICF is in place, a point of contact should be agreed between the ESAs, the ECB, and the relevant authorities in EU Member States: Recommendation of the ESRB of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities (ESRB/2021/17).

All financial institutions should be able to participate in scenario testing and information-sharing. Advanced testing techniques are steadily becoming more embedded. The DORA requirements on advanced testing should incentivise and accelerate the use of threat-led penetration testing. Within the EU, the Framework for Threat Intelligence-based Ethical Red Teaming (TIBER–EU) is the common advanced testing measure. The testing is completed by 'red' teams, following preparatory guidance by 'white team' members of an organisation, as 'blue team' members will be uninformed of the testing. The testing is described as mimicking "the tactics, techniques and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat to entities." [88] In simulating an attack on an entity's critical functions and its underlying systems, the goal is to help an entity "to assess its protection, detection and response capabilities." [89]

In the UK, the equivalent testing framework is the CBEST assessment tool as administered by the Bank of England and the Prudential Regulation Authority (PRA). [90] CBEST incorporates review recommendations on a periodic basis, most recently for revised templates for penetration testing reports. CBEST has sought to differentiate itself from comparable frameworks internationally through its "intelligence-led 'golden thread'", which is orientated towards assessing the traceability of an organisation's role "in supporting the wider economy and the credible threats that the organisation faces in undertaking that role." [91]

If setting the basic apparatus for coordinated testing standards, for information-sharing, and for advanced testing techniques is paramount to mitigating cyber-risks, the mechanisms for reporting of cyber incidents and cyber-attacks are the unresolved next targets. DORA may provide for reporting to a centralised EU hub, but there will be choices to be made as to how the most effective and efficient means of reporting can be accomplished. For the sake of international coordination, data portals for self-executing reports proffer the most likely future example for reporting of cyber incidents and cyber-attacks. As a technological phenomenon, this is nothing new for financial institutions and supervisory authorities. The appeal of

[88] ECB, *TIBER – EU Framework. How to Implement the European Framework for Threat Intelligence-based Ethical Red Teaming* (May 2018), p. 2.
[89] ECB, *TIBER – EU Framework. How to Implement the European Framework for Threat Intelligence-based Ethical Red Teaming* (2018), p. 2.
[90] See the CBEST Threat Intelligence-Led Assessments Implementation Guide for Participants on the Bank of England website at: https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide (date accessed: 27 April 2023).
[91] See Figure 1, Implementation Guide for CBEST Participants.

automated reporting – and the practical and regulatory hindrances to its adoption – is already guiding much of the institutional, policy, and academic discourse on the use of technology for regulatory reporting, compliance and performance of supervisory functions ('RegTech' and 'SupTech'). [92]

In April 2023, the FSB has produced a proposal for a Format for Incident Reporting Exchange (FIRE), [93] which would be automated in nature, enabling machine generated reporting of incidents, and allowing for machine readable/actionable processing of reports between financial institutions and authorities. [94] The merits of the automated FIRE initiative are articulated convincingly by the FSB proposal, but potential risks and costs are also noted. The project could suffer from lack of sponsorship, insufficient adoption levels, a localised mismatch in appetite (such as when an authority decides not to engage with FIRE, but is challenged by a regulated institution), divergent views on FIRE's technical design, and long-term risks concerning its maintenance. Furthermore, there are costs to be incurred in making arrangements for transition or migration to a new reporting exchange system, altering existing regulatory policies and rules, and meeting the costs of entry. [95] At the time of writing, an FSB working group is to be established and will proceed to develop the FIRE system over phases with a two-year duration.

As conceded above, three will be a continuing search for a reporting system which is as genuinely innovative as the cyber-risks that are surfacing in modern finance. An automated portal or exchange seems to be the destination point, but there is progress to be sustained in ensuring international standard-setting and collaboration on testing standards. As explicated in this section, a coordinated approach by financial institutions and supervisory authorities – in formulating internal governance procedures and knowledge-sharing – could prove to be even more practically impactful than legislative provisions.

[92] J. McCarthy, 'The Regulation of RegTech and SupTech in Finance: Ensuring Consistency in Principle and in Practice' (2023) 31(2) *Journal of Financial Regulation and Compliance* 186.
[93] FSB, *Format for Incident Reporting Exchange (FIRE). A Possible Way Forward* (April 2023).
[94] FSB, *Format for Incident Reporting Exchange (FIRE). A Possible Way Forward* (April 2023), p. 7.
[95] FSB, *Format for Incident Reporting Exchange (FIRE). A Possible Way Forward* (April 2023), p. 8.

Conclusion

This article has explored how the operational resilience of IT systems in finance can be affected by the resilience of legal and regulatory frameworks to protect against cyber-risks. The changing cyber-risks and threats to cybersecurity in the aftermath of the COVID-19 pandemic were considered. Whether or not cyber-risks can be always definitively regarded as entirely systemic risks, it was observed that the harm which can be inflicted on critical functions of financial services necessitates an internationalised outlook towards coherent standard-setting. The article portrayed the efforts which are being taken by leading international agencies to formulate cohesive standards for implementation across global finance.

As a prime example of how legislative intervention can impose express requirements on financial entities to address cyber-risks, the EU's DORA Regulation was outlined, with particular emphasis placed on the provisions for ICT risk management, cyber incident reporting, and testing. DORA will serve as an emphatically instructive model for jurisdictions internationally. However, the article examined the significant scope for clarification of testing and reporting standards. By reference to very promising propositions from authorities such as the ESRB and the FSB, the article explained how collaboration and coordination between financial institutions and supervisory authorities will determine the future viability of scenario testing techniques, information-sharing platforms, threat-led penetration testing and other advanced testing methods, and automated reporting portals or exchanges.

Sector-led standards, internal governance procedures, and institutional codes of conduct must be combined with legislative initiatives. Arguments surrounding cyber-risk and systemic risk may occasionally appear somewhat abstract or circular. Nonetheless, it is only by establishing internationally coordinated and resilient standards to diminish cyber-risks that regulators can avoid receiving an unwanted sense of how systemic a cyber-risk can become.