CYBERSECURITY REGULATION IN THE FINANCIAL SECTOR: PROSPECTS OF LEGAL HARMONISATION IN THE EU AND BEYOND

ANTON N DIDENKO

Forthcoming (2020) 1 *Uniform Law Review*
[2020] *UNSWLRS* 9

UNSW Law
UNSW Sydney NSW 2052 Australia

CYBERSECURITY REGULATION IN THE FINANCIAL SECTOR: PROSPECTS OF LEGAL HARMONISATION IN THE EU AND BEYOND

Anton N Didenko[*]

Abstract

Over the past several years, the cybersecurity regulatory landscape has undergone unprecedented change. Bespoke cybersecurity laws and regulations have replaced pre-existing general risk management and business continuity rules in a number of jurisdictions, including the European Union, Hong Kong, Russia, the USA and Singapore. Cybersecurity has also become the focus of international rules and recommendations adopted by numerous international organisations. The financial sector lies at the centre of the new regulatory initiatives – which, in the absence of an agreed international approach, vary substantially across jurisdictions. This article analyses these emerging legal frameworks by (i) conducting a comparative study of the novel cybersecurity regulations in finance, (ii) identifying the common features of such frameworks and (iii) assessing the prospect of their harmonisation at an international level. It argues that international harmonisation in this area is necessary to overcome the underlying regulatory challenges and outlines the scope of rules amenable, first, to initial (*de minimis*) and, second, subsequent (more expansive) harmonisation. The article concludes with a list of main upcoming challenges in designing and harmonising cybersecurity regulations in finance and practical recommendations for overcoming them.

[*] Research Fellow and Member, Centre for Law, Markets and Regulation, UNSW Sydney.

This article has been prepared by the author under the Legal Research Programme sponsored by the European Central Bank (ECB). The author is grateful to the ECB for the comments and suggestions received and acknowledges that any views expressed in this article are only those of the author, and do not necessarily represent the views of the ECB or the Eurosystem. The author also wishes to thank Ross Buckley for his invaluable comments.

Keywords: cybersecurity, regulation, finance, harmonisation, EU (European Union), comparative, Hong Kong, Singapore, Russia, New York

> Going forward, the only thing that's cast in stone is the certainty of future change. And, to embrace this together, we must not see regulation as an adjunct to cyber security, but as a vital part of it.
>
> Marc Bayle de Jessé[1]

I. INTRODUCTION

In the modern digital world, where there is money, there are cyber attackers. According to IBM, the finance and insurance sector has now been the single most attacked industry for three years in a row (with 19 per cent of all recorded attacks in 2018).[2] Hardly surprising, given that 'digital' is the de-facto trend in finance, where digital financial services are seen as one of the key drivers of greater financial inclusion. The 'digital' trend is here to stay, as illustrated by the recent launch of the UN Secretary-General's Task Force on Digital Financing of the Sustainable Development Goals,[3] the promotion of digital financial services

[1] See MB de Jessé, 'ECB Views on the Regulation of Cyber Security' (21 November 2017) 3 <https://www.ecb.europa.eu/paym/intro/news/shared/2017-11-21_cyber_security_regulation.pdf>.

[2] IBM, 'X-Force Threat Intelligence Index 2019' (2019) 16-17 <https://www.ibm.com/downloads/cas/ZGB3ERYD>.

[3] The task force met for the first time in January 2019. Its mandate is 'to identify opportunities, challenges, and ways to advance the convergence of digital technology, the financial ecosystem and the [Sustainable Development Goals]'. See United Nations Secretary-General's Task Force on Digital Financing of the Sustainable Development Goals, 'Harnessing the Digitalization of Finance to Achieve the Sustainable Development Goals' (2019) <https://digitalfinancingtaskforce.org/wp-content/uploads/2019/03/Attachment-1.pdf>.

by international development agencies,[4] the opportunities created by business (both in the developed and developing world)[5] and the interest from academia.[6]

Good progress in overall digitisation of finance has been made over the recent years. Indeed, the World Bank reports that between 2014 and 2017 the number of adults using digital payments increased from 41 to 52 per cent (11 per cent increase)[7] and the share of adults with an account[8] has grown from 62 to 69 per cent (7 per cent increase).[9] This translates into half a billion new users connected to the digital financial infrastructure – as well as *half a billion new targets* for cyber attackers.

Yet, just as cyber-attacks were not invented yesterday, so financial institutions are (or at least should be) aware of potential risks. After all, cybersecurity[10] risk is but one form of operational risk that 'needs to be part of general risk management procedures, of general

[4] See, eg, Office of the United Nations Secretary-General's Special Advocate for Inclusive Finance for Development, Better Than Cash Alliance, United Nations Capital Development and the World Bank, 'Igniting SDG Progress Through Digital Financial Inclusion' (2018) <http://www.uncdf.org/download/file/127/7145/0510180btca-sdg-digitalbookletpdf>; Alliance for Financial Inclusion, 'Digital Financial Services' <https://www.afi-global.org/policy-areas/digital-financial-services>.

[5] See, eg, UNCDF, 'Case Study: How a Microfinance Institution is Reaping the Rewards of Going Paperless in Senegal' (14 June 2018) <https://www.uncdf.org/article/3753/case-study-how-a-microfinance-institution-is-reaping-the-rewards-of-going-paperless-in-senegal>; UNCDF, 'Three Months Down the road: The story of MoKash in Uganda' (20 November 2017) <https://www.uncdf.org/article/1675/three-months-down-the-road-the-story-of-mokash-in-uganda-migration>.

[6] The author is partly responsible as well. See, eg, [author's other publications in the area – edited out for blind peer review purposes].

[7] A Demirgüç-Kunt et al, 'The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution' (2018) 55 <http://documents.worldbank.org/curated/en/332881525873182837/pdf/126033-PUB-PUBLIC-pubdate-4-19-2018.pdf>.

[8] That is users who 'opened an account at a financial institution or through a mobile money provider'. See ibid 2.

[9] ibid 2.

[10] The Financial Stability Board defines the term as 'preservation of *confidentiality*, *integrity* and *availability* of information and/or *information systems* through the *cyber* medium'. See Financial Stability Board, 'Cyber Lexicon' (2018) 9 <https://www.fsb.org/wp-content/uploads/P121118-1.pdf>.

crisis management, and general business continuity planning'.[11] However, until recently, rules relating to cyber-resilience[12] rarely took the form of dedicated cybersecurity instruments and instead were generally included into other regulations (eg on data protection) – and, for this reason, often remained rudimentary.

Over the past several years, the cybersecurity regulatory landscape has undergone substantial changes. New laws and regulatory instruments focusing exclusively on cyber-resilience have been adopted in a number of jurisdictions, including Hong Kong, Russia, the USA and Singapore. Cybersecurity has also become the focus of international rules and recommendations adopted by numerous organisations, including the BCBS, CPMI, FSB, G7, IAIS, IMF, IOSCO, OECD and the World Bank Group (see section V(A) below for more details). Nonetheless, the apparently high interest in possible international harmonisation of cybersecurity regulatory regimes has not yet translated into hard international law.

The financial sector lies at the centre of the new cybersecurity instruments, which emerged as a result of convergence of multiple factors (discussed in section II below). However, in the absence of an agreed international approach, the new cybersecurity rules vary significantly across jurisdictions. This article analyses the emerging legal frameworks in the area of cybersecurity in finance by conducting a comparative study covering the legal systems in Europe, Asia, North America and Australia. It identifies the common features of such frameworks and assesses the prospect of their harmonisation at an international level. Since cybersecurity frameworks differ dramatically across the selected jurisdictions (making a straight side-by-side comparison counterintuitive), both in terms of scope and level of

[11] S Lautenschläger, 'Cyber resilience – objectives and tools' (9 March 2018) <https://www.bankingsupervision.europa.eu/press/speeches/date/2018/html/ssm.sp180309.en.html>.

[12] The term refers to 'the ability of an organisation to continue to carry out its mission by anticipating and adapting to *cyber threat*s and other relevant changes in the environment and by withstanding, containing and rapidly recovering from *cyber incident*s'. See Financial Stability Board, 'Cyber Lexicon' (2018) (n 10) 9.

detail, the primary focus of this article is on the only known transnational system of cybersecurity rules – legislation and regulations adopted at the European Union (EU) level – as a possible early precursor to broader international harmonisation.[13]

For practical reasons, this study is limited in several ways. First, it is based on publicly available regulations.[14] Second, it analyses only regulations adopted in, or relevant for, the financial services sector. Third, this article does not tackle any aspects of criminal liability for cyber offences or criminal law in general.

The remainder of this article is structured as follows. Section II explains the main reasons for the increasing regulatory attention to cybersecurity in the financial sector. Section III outlines the different levels of cybersecurity regulation in the EU. Section IV highlights the evolving nature of cybersecurity regulation. Sections V and VI analyse, respectively, the prospect and scope of legal harmonisation of cybersecurity regulation in finance. Section VII concludes the article and outlines the key challenges and lessons for future legal harmonisation in the area.

II. REASONS FOR INCREASING REGULATORY ATTENTION

Several factors can explain why the new cybersecurity regulations focus on the financial sector.

First, cyber-threats demand an entirely different ('assume breach') attitude, based on the realistic assumption that not all attacks can be prevented, and thus more emphasis should be put on identifying – and responding to – threats, rather than attempting to build

[13] While individual Member State rules and regulations are also considered to highlight relevant points, their analysis is beyond the scope of this article.

[14] In this article, 'regulation' is understood in the broad sense as formal rules and recommendations made by a government or other authority (whether domestic or international) in order to control the way something is done, or the way people behave. The word 'formal' implies that any informal measures (such as industry self-regulation or market forces and customs) are excluded.

impenetrable cyber-fortresses. This approach is driven, among other factors, by the different nature of cyber threats (which are persistent, dynamic, intelligent and adaptive),[15] their ability to easily penetrate national borders and the inefficiency of certain measures to prevent operational disruption (such as mirroring of data on a server in a different physical location) in addressing them. Coupled with their (invariably) stealthy nature and the ability to escalate quickly, these factors make cyber-attacks a real danger.

Second, the financial sector is undergoing an unprecedented increase in digitisation of data. Examples include (i) direct secure digital channels of communication with central banks, (ii) new methods of payment within payment systems (eg using bar codes, phone numbers or wearable tech), (iii) paperless documentary operations (including those implementing distributed ledger technology), (iv) implementation of 'smart contracts', (v) increasing use of biometric data to identify clients of financial institutions (from the ambitious Aadhaar project in India, to the new biometric platform for bank client identification in Russia) and (vi) new bank reporting formats. The trend is only going to continue with the proliferation of big data, since, as the CFTC Chairman Christopher Giancarlo eloquently put it during the announcement of the new office of data and analytics in November 2018, 'if data is King, then automating processes which previously required…human effort is the critical work of the King's Court'.[16]

Third, increasing complexity and interconnectedness of the financial ecosystem – based on the interdependent operational network of a broad range of actors (banks, financial market

[15] These characteristics stem from the nature of the source of cyber threats – motivated, and often sophisticated, attackers. See BIS Committee on Payments and Market Infrastructures and International Organisation of Securities Commissions, 'Guidance on Cyber Resilience for Financial Market Infrastructures' (2016) 4 <https://www.bis.org/cpmi/publ/d146.pdf>.

[16] US Commodity Futures Trading Commission, 'Quantitative Regulation: Effective Market Regulation in a Digital Era' (07 November 2018) <https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo59>.

infrastructures, various service providers) – increases the risks of contagion and creates new entry points for attackers, thus calling for greater overall cybersecurity within the entire financial sector (and not just the largest institutions). Increasing integration of new types of third party services (eg by cloud service providers, which store data outside regulated financial institutions) further increases these risks.

Fourth, the cost of cyber-attacks in the financial sector is very high. According to Accenture, the banking sector experienced the highest average annual cost of cybercrime in 2018 (at over USD 18 million per bank), with insurance in fifth place (at over USD 15 million per company).[17] Since the cost is likely to be passed on to customers, regulators are likely to have an interest in reducing the impact of cyber-attacks.

Fifth, past events have made it very clear that neither the biggest financial institutions, nor financial regulators are immune to cyber threats:[18] the central banks of Azerbaijan, Bangladesh, Ecuador, Italy, Russia, Sweden and the US, as well as the ECB, have all been victims of successful cyber-attacks in recent years.[19]

III. LAYERS OF CYBERSECURITY REGULATION IN THE EU

Cybersecurity rules in the EU affecting the financial sector are spread across dozens of instruments (some of which are sector-specific, while others remain sector-neutral). These instruments are analysed in sections III.1 and III.2.

---

[17] Accenture Security and Ponemon Institute, 'The Cost of Cybercrime' (Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection, 2019) 12 <https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50>.

[18] See MB de Jessé (n 1) 1.

[19] A Bouveret, 'Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment' (IMF Working Paper, 2018) 8-9 <https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx>.

A. Cybersecurity Strategy and Cross-sector Rules

At the EU level,[20] the origins of bespoke cybersecurity regulation can be traced back to 2013 and the publication of the Cybersecurity Strategy.[21] The document outlined the EU's overall vision in this area, allocated responsibilities and listed actions required (rather ambitiously) 'to make the EU's online environment the safest in the world'.[22] In doing so, the Cybersecurity Strategy aspired to have extraterritorial impact, by stating principles 'that should guide cybersecurity policy in the EU and *internationally*'.[23] Ultimately, five strategic priorities were put forward: (i) achieving cyber resilience, (ii) drastically reducing cybercrime, (iii) developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP), (iv) developing the industrial and technological resources for cybersecurity and (v) establishing a coherent international cyberspace policy. The complexity of the cybersecurity field and variety of stakeholders involved in this area prompted the conclusion that, 'centralised … European supervision is not the answer'[24] and that a combination of national and supranational action (at EU level) would be most effective, as illustrated in the following image.

Image 1. Main cybersecurity actors and levels of regulation in the EU Cybersecurity Strategy[25]

[20] Individual Member States regulate cybersecurity at a domestic level as well, but analysis of national cybersecurity regulation of EU Member States is beyond the scope of this article.

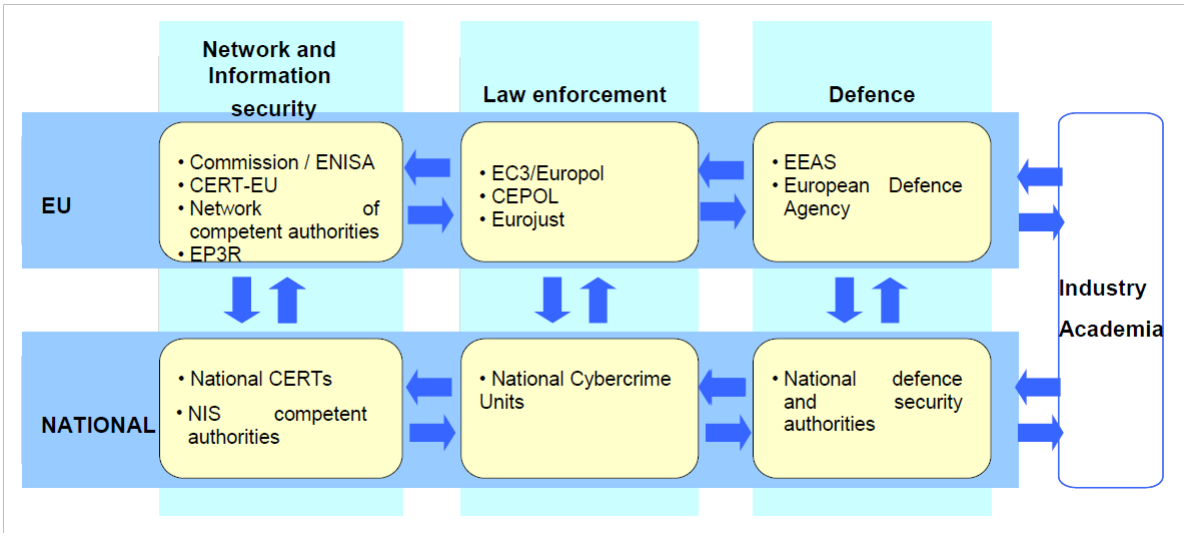
[21] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' (2013) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667>.

[22] ibid 3.

[23] ibid 3 (emphasis added). These principles are as follows: (i) the EU's core values to apply as much in the digital as in the physical world, (ii) protecting fundamental rights, freedom of expression, personal data and privacy, (iii) Internet access for all, (iv) democratic and efficient multi-stakeholder governance, and (v) shared responsibility to ensure cybersecurity. See ibid 3-4.

[24] ibid 17.

[25] ibid.



The Cybersecurity Strategy was accompanied by a proposal for a new directive on security of network and information systems (NIS) – an instrument aiming 'to ensure a high common level of network and information security' in the EU.[26] Although the instrument was meant to apply to a range of industries, it signalled a transition to greater overall regulatory intervention into the cybersecurity space, based on the conclusion that the 'purely voluntary approach… does not provide sufficient protection against NIS incidents and risks across the EU'.[27] Unsurprisingly, the broad scope of the proposed NIS Directive raised the issue of possible overlaps with other, industry-specific rules. In particular, in the context of the financial sector, the European Central Bank (ECB) issued a legal opinion suggesting that the NIS Directive should apply 'without prejudice to the existing regime for the Eurosystem's oversight of payment and settlement systems', highlighting the vested interest of financial regulators, in particular the ECB, the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA).[28] Interestingly, the final text of the NIS Directive,

[26] European Commission, 'Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union' (COM(2013) 48 final, 2013/0027 (COD)) 1.

[27] ibid 3.

[28] European Central Bank, 'Opinion of the European Central Bank of 25 July 2014 on a Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High

which was adopted in 2016, attempts to address the issue by making it clear that the document sets only the baseline standards for NIS security that may be overridden by sector-specific EU rules imposing equal or higher requirements:

> Where a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are *at least equivalent* in effect to the obligations laid down in this Directive, those provisions of that sector-specific Union legal act shall apply.[29]

A massive increase in the impact of cyber-attacks in recent years has led to a proposal for further revision of the cybersecurity regulatory framework across three dimensions: (i) building EU resilience to cyber-attacks, (ii) creating effective EU cyber deterrence and (iii) strengthening international cooperation on cybersecurity.[30] The proposal was accompanied by a draft regulation (known as 'Cybersecurity Act')[31] to enhance the mandate of ENISA[32] as

---

Common Level of Network and Information Security Across the Union (CON/2014/58) (OJ C 352/4) paras 2-3.

[29] Directive (EU) 2016/1148 of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (OJ L 194/1) art 1(7) (NIS Directive) (emphasis added).

[30] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 'Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU' (2017) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en> accessed 07 June 2019.

[31] The instrument was adopted in its final form in April 2019. See Regulation (EU) 2019/881 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 (Cybersecurity Act) (OJ L 151/15).

[32] ENISA, abbreviated from European Network and Information Security Agency, was initially established in 2004 for a period of five years with the objective of enhancing the EU capability to 'address and to respond to network and information security problems'. See Articles 2, 27 of the Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency (OJ L 77/1).

an independent centre of expertise on cybersecurity in the EU and to establish a European cybersecurity certification framework.[33]

In May 2018, the ECB issued an EU-wide cybersecurity threat-led penetration testing framework known as 'TIBER-EU'.[34] The framework involves 'the use of a variety of techniques to simulate an attack on an entity's critical functions … and underlying systems (i.e. its people, processes and technologies)'[35] and was inspired by national initiatives, such as CBEST in the United Kingdom or TIBER-NL in the Netherlands. Although, in principle, TIBER-EU is sector-neutral and can be used 'for any type or size of entity', it was clearly designed for use in businesses forming the 'core *financial* infrastructure'.[36] In the EU context, the ECB document is unique in that it is developed with a cross-jurisdictional approach in mind whereby threat-led penetration testing is managed by regulators from different countries. At the time of publication, TIBER-EU is applied on a voluntary basis only and its benefits depend entirely on its level of adoption by the relevant EU authorities or individual Member States (which may make participation of certain entities in this framework mandatory).[37]

[33] Cybersecurity Act (n 31), Titles II and III.

[34] European Central Bank, 'TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-based Ethical Red Teaming' (2018) <https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf>.

[35] ibid 2.

[36] ibid 3 (emphasis added). The focus on the financial services market is also clear from the definition of 'entities' covered by the framework, which means 'payment systems, central securities depositories, central counterparty clearing houses, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies and any other service providers deemed critical for the functioning of the financial sector'. See ibid 7.

[37] ibid 16.

Cybersecurity provisions can also be found in instruments targeting data-intensive businesses and functions. For example, the GDPR,[38] in addition to setting out in detail the regime for the processing of personal data and rules relating to the free movement of personal data, imposes explicit obligations to ensure security of data processing (Article 32) and duties to give *ex post* notice of a data breach to the competent authorities (Article 33) and to the data subject (Article 34). Similarly, the eIDAS Regulation[39] sets out security requirements applicable to trust service providers (Article 19).

B. Cybersecurity in Finance

In finance, there are at least eight different sets of cybersecurity rules and regulations operating at the EU level.[40] These are as follows.

First, *credit institutions and investment firms* are subject to dedicated operational risk[41] requirements. These include own funds requirements,[42] the duty to have in place policies and processes to evaluate and manage operational risk exposure,[43] as well as contingency and

[38] Regulation (EU) 2016/679 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) (OJ L 119/1). For the sake of completeness, it should be noted that the GDPR applies to processing of personal data 'whether or not by automated means' (Article 4(2)).

[39] Regulation (EU) No 910/2014 of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC (OJ L 257/73).

[40] The co-existence of sectoral (financial) and cross-sectoral cybersecurity rules creates a sophisticated regulatory framework that is prone to overlaps. As a result, the seemingly straightforward diagram in Image 1 above becomes substantially more complex, providing an incentive for harmonisation of cybersecurity regimes, but nationally and on cross-border basis.

[41] Defined as 'risk of loss resulting from inadequate or failed internal processes, people and systems or from external events', which is broad enough to incorporate all forms of cyber risks. See Article 4(1)(52) of Regulation (EU) No 575/2013 of 26 June 2013 on Prudential Requirements for Credit Institutions and Investment Firms and Amending Regulation (EU) No 648/2012 (OJ 176/1).

[42] Regulation (EU) No 575/2013 (n 41), Part Three, Title III ('Own Funds Requirements for Operational Risk').

[43] Directive 2013/36/EU of 26 June 2013 on Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms, Amending Directive 2002/87/EC and Repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176/338), Article 85(1).

business continuity plans in the event of severe business disruption.[44] Since July 2017, banks directly supervised by the ECB are subject to cyber event reporting requirements imposed by the European banking regulator.[45]

Second, the Payment Services Directive (PSD2) requires *payment service providers* to establish frameworks with mitigation and control mechanisms for managing 'operational and security risks'[46] and to report major operational or security incidents.[47] In addition, the EBA and the ECB were empowered to develop various supplementary instruments: (i) guidelines on security measures,[48] (ii) corresponding draft regulatory technical standards,[49] (iii) major incident reporting guidelines[50] and (iv) technical standards on authentication and communication.[51] Finally, in furtherance of Article 96(6) of PSD2, the EBA adopted its guidelines on fraud data reporting.[52]

---

[44] ibid, Article 85(2).

[45] See European Central Bank, 'IT and cyber risk – the SSM perspective' (13 February 2019) <www.bankingsupervision.europa.eu/press/publications/newsletter/2019/html/ssm.nl190213_4.en.html>.

[46] Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337/35), Article 95(1) (emphasis added).

[47] ibid, Article 96(1).

[48] ibid, Article 95(3). In response, the EBA published its Guidelines on the Security Measures for Operational and Security Risks of Payment Services under Directive (EU) 2015/2366 (PSD2) <https://eba.europa.eu/documents/10180/2081899/Guidelines+on+the+security+measures+under+PSD2+%28EBA-GL-2017-17%29_EN.pdf/c63cfcbf-7412-4cfb-8e07-47a05d016417>.

[49] ibid, Article 95(4).

[50] ibid, Article 96(3). This led to the development of the EBA Guidelines on Major Incident Reporting under Directive (EU) 2015/2366 (PSD2) <https://eba.europa.eu/documents/10180/2066978/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29_EN.zip/851a7e22-0900-4c64-8710-2fbe30a15cb3>.

[51] ibid, Article 98(4). See EBA, Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2) <https://eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf>. The EBA document was used as a basis for Regulation (EU) 2018/389 of 27 November 2017 Supplementing Directive (EU) 2015/2366 with Regard to Regulatory

Third, the ECB has adopted the SIPS Regulation, which is a set of oversight requirements for *systemically important payment systems (SIPS)*. These rules require each SIPS operator to establish 'a robust framework … to identify, monitor and manage operational risk'.[53] More specifically, SIPS operators must set up 'comprehensive physical and information security policies that adequately identify, assess and manage all potential vulnerabilities and threats',[54] prepare a business continuity plan in case of operational disruptions[55] and identify, and manage, the risks of third parties, including critical SIPS participants whose operational disruption may impact SIPS functioning.[56] In 2017 the SIPS Regulation was amended by the ECB to incorporate new international guidance (see section V(A) below).[57]

Retail payment systems are subject to the Revised Oversight Framework for Retail Payment Systems with similar provisions relating to operational risk.[58]

Finally, in December 2018, the ECB published its Cyber Resilience Oversight Expectations for Financial Market Infrastructures (CROE).[59] The CROE directly apply to

---

Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication (OJ L 69/23).

[52] See EBA Guidelines on reporting requirements for fraud data under Article 96(6) PSD2 <https://eba.europa.eu/documents/10180/2352765/Guidelines+on+fraud+reporting+%28EBA+GL-2018-05%29_EN.pdf/f84b2ec7-6ddf-4c12-bd02-59aa4a99f1f0>.

[53] Regulation of The European Central Bank (EU) No 795/2014 of 3 July 2014 on Oversight Requirements for Systemically Important Payment Systems (OJ L 217/16), Article 15(1).

[54] ibid, Article 15(4).

[55] ibid, Article 15(5).

[56] ibid, Articles 15(6)-15(7).

[57] ECB, Regulation (EU) 2017/2094 of the European Central Bank of 3 November 2017 Amending Regulation (EU) No 795/2014 on Oversight Requirements for Systemically Important Payment Systems (ECB/2017/32) <https://www.ecb.europa.eu/ecb/legal/pdf/celex_32017r2094_en_txt.pdf>.

[58] ECB, Revised Oversight Framework for Retail Payment Systems <https://www.ecb.europa.eu/pub/pdf/other/Revised_oversight_framework_for_retail_payment_systems.pdf>.

entities over which Eurosystem[60] has competence (namely payment systems and T2S),[61] but can be implemented by the competent national regulators to apply to other FMIs, such as securities settlement systems, central securities depositories and central counterparties (CCP).

Fourth, *trade repositories* are subject to operational risk requirements under EMIR, which requires that the systems used must be 'reliable and secure'.[62] An adequate business continuity policy and disaster recovery plan must be implemented and should 'at least provide for the establishment of backup facilities'.[63] More detailed requirements for the design and operation of information technology systems have been developed under EMIR for *CCPs*, including an obligation to 'base [such systems] on internationally recognised technical standards and industry best practices'.[64]

Fifth, under the Solvency II directive, *insurance and reinsurance undertakings* are required to have in place risk management systems covering, among other things, operational risks[65] – in addition to adequate minimum capital.[66] The requirements in respect of

---

[59] European Central Bank, Cyber Resilience Oversight Expectations for Financial Market Infrastructures' (2018) <https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf>.

[60] The Eurosystem comprises 'the European Central Bank, together with the national central banks of the Member States whose currency is the euro'. See Article 282(1) of the Treaty on the Functioning of the European Union (consolidated version).

[61] Different levels of cyber maturity are expected from different payment systems: see section VI(B) below.

[62] Regulation (EU) No 648/2012 of 4 July 2012 on OTC Derivatives, Central Counterparties and Trade Repositories (OJ L 201/1) (EMIR), Article 79(1).

[63] ibid, Article 79(2).

[64] Regulation (EU) No 153/2013 of 19 December 2012 supplementing Regulation (EU) No 648/2012 with Regard to Regulatory Technical Standards on Requirements for Central Counterparties (OJ L 52/41), Article 9.

[65] Directive 2009/138/EC of 25 November 2009 on the Taking-up and Pursuit of the Business of Insurance and Reinsurance (Solvency II) (OJ L 335/1), Article 44(2)(e).

[66] ibid, Article 107. See also Regulation (EU) 2015/35 of 10 October 2014 Supplementing Directive 2009/138/EC of the European Parliament and of the Council on the Taking-up and Pursuit of the Business of Insurance and Reinsurance (Solvency II) (OJ L 12/1), Section 8 ('Operational Risk').

operational risk management policy are further clarified by the European Insurance and Occupational Pensions Authority (EIOPA).[67]

Sixth, *credit rating agencies* are required to have 'effective control and safeguard arrangements for information processing systems'.[68]

Seventh, a broad range of operational risk requirements apply to *central securities depositories* (CSD), including obligations to (i) maintain 'IT tools that ensure a high degree of security',[69] (ii) have 'adequate business continuity policy and disaster recovery plan' (including the setting up of a second processing site),[70] (iii) organise a testing programme[71] and (iv) 'identify, monitor and manage the risks that key [CSD participants], as well as service and utility providers, and other CSDs or other market infrastructures might pose to … operations'.[72] CSDs are also subject to dedicated capital requirements for operational risks.[73]

[67] See Guideline 21 'Operational Risk Management Policy' in EIOPA Guidelines on System of Governance (EIOPA-BoS-14/253 EN) <https://eiopa.europa.eu/GuidelinesSII/EIOPA-BoS-14-253_GL%20on%20system%20of%20governance.pdf>.

[68] Regulation (EC) No 1060/2009 of 16 September 2009 on Credit Rating Agencies (OJ L 302/1), Annex I, s 4. See also the amending instrument – Regulation (EU) No 462/2013 of 21 May 2013 Amending Regulation (EC) No 1060/2009 on Credit Rating Agencies <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:146:0001:0033:EN:PDF>. See also Commission Delegated Regulation (EU) No 449/2012 of 21 March 2012 Supplementing Regulation (EC) No 1060/2009 of the European Parliament and of the Council with Regard to Regulatory Technical Standards on Information for Registration and Certification of Credit Rating Agencies <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0449&from=EN>.

[69] Regulation (EU) No 909/2014 of 23 July 2014 on Improving Securities Settlement in the European Union and on Central Securities Depositories and Amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L 2571), Article 45(2).

[70] ibid, Article 45(3)-45(4).

[71] ibid, Article 45(5).

[72] ibid, Article 45(6).

[73] ibid, Article 47. Regulation (EU) 2017/390 of 11 November 2016 Supplementing Regulation (EU) No 909/2014 with Regard to Regulatory Technical Standards on Certain Prudential Requirements for Central Securities Depositories and Designated Credit Institutions Offering Banking-type Ancillary Services, Article 4.

Eighth, MiFID II[74] and MiFIR[75] impose a set of requirements applicable to parties engaged in trading regulated financial instruments, such as *investment firms*, *trading venues* and *data reporting services providers*[76]. Investment firms are required to have 'effective control and safeguard arrangements for information processing systems', as well as 'sound security mechanisms … to guarantee the security and authentication of the means of transfer of information, minimise the risk of data corruption and unauthorised access and to prevent information leakage'.[77] Additional requirements apply to investment firms engaged in algorithmic trading, such as an obligation to have 'effective systems and risk controls to ensure the trading systems cannot be used for any purpose … contrary to [market abuse rules] or to the rules of a trading venue to which it is connected'[78] and a duty to undertake annual penetration tests and vulnerability scans to simulate cyber-attacks.[79] Trading venues[80] and data reporting services providers[81] are subject to their own requirements.

In addition, the need for enhanced cybersecurity regulation features prominently in the European Commission's 2018 FinTech Action Plan, which proclaims:

[74] Directive 2014/65/EU of 15 May 2014 on Markets in Financial Instruments and Amending Directive 2002/92/EC and Directive 2011/61/EU (recast) (OJ L 173/349).

[75] Regulation (EU) No 600/2014 of 15 May 2014 on Markets in Financial Instruments.

[76] These include approved publication arrangements (APAs), consolidated tape providers (CTPs), approved reporting mechanisms (ARMs).

[77] Directive 2014/65/EU of 15 May 2014 on Markets in Financial Instruments and Amending Directive 2002/92/EC and Directive 2011/61/EU (recast) (OJ L 173/349), Article 16(5).

[78] ibid, Article 17(1).

[79] Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU with Regard to Regulatory Technical Standards Specifying the Organisational Requirements of Investment Firms Engaged in Algorithmic Trading (OJ L 87/417), Article 18(4).

[80] See Regulation (EU) No 600/2014 of 15 May 2014 on Markets in Financial Instruments and Amending Regulation (EU) No 648/2012 (OJ L 173/84), Article 26(7); Regulation (EU) 2017/584 of 14 July 2016 Supplementing Directive 2014/65/EU with regard to Regulatory Technical Standards Specifying Organisational Requirements of Trading Venues (OJ L 87/350), Article 23; MiFID II, Article 48(1).

[81] See MiFID II, Articles 64(4), 65(5), 66(3).

> Making the financial sector more cyber resilient is of paramount importance to ensure that it is well protected, that financial services are delivered effectively and smoothly across the EU, and that consumer and market trust and confidence are preserved.[82]

IV. EVOLVING DESIGN OF CYBERSECURITY REGULATION

The outline, in the previous section, of key EU regulations highlights the ongoing decoupling of cybersecurity rules from general operational risk management provisions in addition to the increasing sophistication of the regulatory regime. This trend can be observed in a number of jurisdictions (such as Hong Kong, Russia, Singapore and the USA) and stems from acknowledging the unique characteristics of cyber threats demanding a more elaborate approach to tackle them efficiently.[83] Nonetheless, the same unique characteristics require regulators to take a different approach, by encouraging flexibility and continuous improvement of cybersecurity measures to avoid playing catch up with the development of technology (a game regulators are not always good at, to say the least). As a result, cyber rules often end up focusing largely on procedural requirements (such as the need to have a corresponding corporate strategy to address cyber risks).

A. Uncertainty through Obscurity

Most jurisdictions today address cybersecurity matters as part of IT or operational risk rules and regulations.[84] While there can be no doubt that cybersecurity risks are a subset of operational risks, regulation often fails to adequately distinguish the two and applies a one-

[82] European Commission, 'FinTech Action plan: For a more competitive and innovative European financial sector' (2018) 3 <https://eur-lex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73-01aa75ed71a1.0001.02/DOC_1&format=PDF>.

[83] See section II above.

[84] Basel Committee on Banking Supervision, 'Cyber-Resilience: Range of Practices' (2018) 9 <https://www.bis.org/bcbs/publ/d454.pdf>.

size-fits-all approach. For example, capital requirements for operational risk do not distinguish the 'cyber' element.[85] The same can be said about general duties to have in place 'policies and processes to evaluate and manage the exposure to operational risk'[86] or to 'identify sources of operational risk and minimise them'.[87]

Even when cybersecurity and operational risk matters are formally separated, the rules may remain broad and obscure. In some cases, separation is only textual, with no impact on the scope or interpretation of the relevant rules. For example, PSD2 refers to 'operational and security risks' throughout Article 95 but the difference between the two risk types is vague at best.

Regardless of any formal separation from other types of operational matters, cybersecurity regulation often remains principles-based, resulting in obscure, abstract, high level requirements essentially telling regulated entities to 'do the right thing' while omitting to explain what exactly that entails. A common formula found in many EU instruments includes two related obligations, one addressing ongoing duties and the other specifying the desirable end-result: (i) an obligation to take *appropriate* technical and organisational *measures* to manage cyber risks, and (ii) an obligation to achieve a *level* of security *appropriate* to the risks. For example, such provisions are found in the eIDAS Regulation,[88] NIS Directive[89] or the GDPR.[90]

[85] See, eg, Regulation (EU) No 575/2013 (n 41), Part Three, Title III; Solvency II Directive (n 65), Article 107; Regulation (EU) No 909/2014 (n 69), Article 47; Regulation (EU) 2017/390 (n 73), Article 4.

[86] Directive 2013/36/EU (n 43), Article 85(1).

[87] EMIR (n 62), Article 79(1).

[88] eIDAS (n 39), Article 19(1).

[89] NIS Directive (n 29), Articles 14(1) and 16(1).

[90] GDPR (n 38), Article 32(1).

Although the wording of various provisions may vary (often with little change in meaning), more specific cybersecurity rules are rare. For example, in the GDPR, which imposes a duty to implement 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk',[91] the clarifications and more specific requirements that follow later in the text[92] do not eliminate the issue. First, those measures are only given as examples (which is clear from the words 'including inter alia as appropriate'), and their implementation does not guarantee compliance. Second, the recommended measures are themselves vague and uncertain (eg the requirement to 'ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services' can be translated essentially as 'ensure good cybersecurity').[93] In the NIS Directive, the clarification is somewhat more specific: the relevant 'technical and organisational measures' taken by service providers must 'take into account' five elements ((i) security of systems and facilities, (ii) incident handling, (iii) business continuity management, (iv) monitoring, auditing and testing and (v) compliance with international standards).[94] Overall, however, little can be said about the content of these elements, except that they need to be considered in some way.

The implication of a principles-based approach is clear: fear of overregulation and inflexibility of setting out in advance the 'final destination' of a cybersecurity regime that may shift unexpectedly for reasons such as advances in technology. On the one hand, a set of overly prescriptive rules can backfire by providing potential attackers with information about cybersecurity controls implemented across the industry, effectively informing attackers on what must be done to circumvent those controls. On the other hand, regulated firms are very

[91] ibid.

[92] ibid, Article 32(1)(a)-(d).

[93] ibid, Article 32(1)(b).

[94] NIS Directive (n 29), Article 16(1)(a)-(e).

different in terms of their size, systemic importance and technology applied, which demands a certain level of regulatory flexibility. These factors create a major challenge for regulators.

However, vague and uncertain requirements entail another risk: they can be interpreted broadly and narrowly at the same time. When coupled with hefty sanctions for non-compliance (such as those in Article 83(4)(a) of the GDPR), obscure non-specific rules can be seen as an ever-present Sword of Damocles with no prospect of guaranteeing compliance by the regulated entities (which are likely to prefer a regulatory standard ascertainable on an *ex ante* basis).

B. Cyber Governance–

As the level of regulatory sophistication increases, so do cybersecurity rules become more detailed and explicit. A prominent feature of bespoke cybersecurity legal regimes emerging in recent years is their focus on organisational matters, ie cyber governance.[95] Organisational matters are rarely specific as to the end-result and thus, when detailed in cybersecurity regulations, focus on clarifying the steps necessary to achieve the desirable cyber standard and other aspects of procedural character. In EU financial regulation, one of the most recent examples is the CROE, which require each relevant FMI, as a minimum, (i) to 'document its cyber resilience strategy',[96] (ii) to have a 'cyber resilience framework' setting out cyber resilience objectives, risk tolerance and risk management practices,[97] and (iii) appropriate board-level expertise, responsibility and accountability for cybersecurity.[98]

[95] The main areas of cyber governance are: (i) cybersecurity strategy, (ii) management roles and responsibilities, (iii) cyber risk awareness culture, (iv) architecture and standards, and (v) cybersecurity workforce. See Basel Committee on Banking Supervision (n 84) 11.

[96] CROE (n 59), s 2.1.2.1(2).

[97] Ibid, s 2.1.2.1(6).

[98] Ibid, s 2.1.2.2.

Cyber governance is designed not only to allocate responsibility internally, but, importantly, to enable a forward-looking, proactive approach to cybersecurity. It is a core element of cybersecurity design featuring in international guidelines, such as those issued by the G7[99] or the 2016 CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures.[100] Importantly, it is now being increasingly implemented in national regulatory regimes, particularly in the financial sector, albeit sometimes with different terminology. For example, the Cybersecurity Requirements for Financial Services Companies adopted by the New York State Department of Financial Services (NYCRR 500) require regulated entities to maintain a 'cybersecurity *program*'[101] and a 'cybersecurity *policy*'.[102]

A prominent feature that appears to be gaining popularity among regulators is the requirement to appoint a senior executive (often referred to as 'chief information security officer', or 'CISO') to ensure appropriate implementation of cybersecurity strategies or programs – in a sense, a link between the firm's board and the rest of its cybersecurity environment. In this context, the differences between jurisdictions in approaching the matter are not only textual, and evidence multiple design options available. For instance, in the CROE the CISO must be appointed in-house (or, in a group setting, at least on a group-wide basis),[103] whereas the New York regulators allow financial services firms to use a CISO employed by an unaffiliated third-party service provider.[104]

---

[99] G7, 'G7 Fundamental Elements of Cybersecurity for the Financial Sector' (2016), Element 1 and Element 2 <https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf>.

[100] BIS Committee on Payments and Market Infrastructures and International Organisation of Securities Commissions (n 15) 9-10.

[101] NYCRR 500, s 500.02 (emphasis added).

[102] ibid, s 500.03 (emphasis added).

[103] CROE (n 59) 62.

[104] NYCRR 500, s 500.04(a).

The organisational nature of cyber governance implies that the key asset in maintaining cybersecurity is the workforce – and not just the senior management, but staff at all levels. For this reason, modern cyber governance instruments implement additional rules to address this aspect. The scope of the relevant rules can vary a lot, from the most basic provisions to detailed guidance for staff at different levels. The NYCRR 500 are an example of the former approach: the document requires each covered entity to (i) 'utilize qualified cybersecurity personnel' sufficient to manage cyber risks, (ii) 'provide cybersecurity personnel with cybersecurity updates and training' sufficient to address those risks and (iii) ensure that key personnel 'take steps to maintain current knowledge of changing cybersecurity threats and countermeasures'.[105] In contrast, the CROE are much more specific, as they call for: (i) as a minimum, a 'programme for continuing cyber resilience training and skills development for all staff' conducted at least on an annual basis[106] and measures to improve overall cybersecurity culture (eg distribution of situational awareness materials),[107] (ii) at the medium level of expectation, incentives for staff to ensure cyber compliance,[108] 'a programme for talent recruitment, retention and succession planning for the staff'[109] as well as 'well-defined plans for the succession of high-risk staff' in the area of cybersecurity (such as senior management, system administrators or software developers).[110] At the highest level of expectation, the CROE envisages the high-end, proactive cybersecurity organisational efforts: cooperation with other stakeholders to 'promote a cyber resilience culture across the

[105] NYCRR 500, s 500.10(a). See also ibid, s 500.14(b).

[106] CROE (n 59), s 2.1.2.2(27).

[107] ibid, s 2.1.2.2(24-26).

[108] ibid, s 2.1.2.2(34).

[109] ibid, s 2.1.2.2(38).

[110] ibid, s 2.1.2.2(39).

ecosystem'[111] and regular benchmarking internal cybersecurity capabilities against the market to identify deficiencies.[112]

C. Cyber Defences

Although humans and processes stand at the centre of a cybersecurity framework, solid governance alone cannot protect against attacks utilising state of the art technology as effectively as against 'human factor' vulnerabilities (such as employees stealing customer data,[113] or computer administrators misconfiguring a server[114]). For this reason, cybersecurity regulations implement a range of requirements aiming to enhance logical and physical security of relevant systems. Levels of specificity of such rules can vary significantly across jurisdictions and cannot be fully addressed in this article, but several examples will be given for illustrative purposes.

At the EU level, specific (especially technology-related) requirements remain rare, and guidance is largely organisational and principles-based. Even where specific cyber defences are mentioned, they are generally given as examples, rather than mandatory requirements. For example, although Article 32(1) of the GDPR mentions 'pseudonymisation and encryption' of personal data, these two measures must be used alongside others 'as appropriate', which implies that in certain circumstances alternative defences can be used.

[111] ibid, s 2.1.2.2(44), 2.1.2.2(46).

[112] ibid, s 2.1.2.2(45).

[113] In April 2018, SunTrust Banks, Inc announced issued a warning of a 'potential theft by a former employee of information from some of its contact lists'. See SunTrust, 'SunTrust to Offer Free Identity Protection' (2018) <http://newsroom.suntrust.com/2018-04-20-SunTrust-to-Offer-Free-Identity-Protection>.

[114] In September 2018, it was announced that Government Payment Service Inc, a company used by state and local governments to accept online payments leaked more than 14 million customer records due to poorly configured security settings: 'it was possible to view … customer records simply by altering digits in the Web address displayed by each receipt'. See KrebsOnSecurity, 'GovPayNow.com Leaks 14M+ Records' (2018) <https://krebsonsecurity.com/2018/09/govpaynow-com-leaks-14m-records/>.

The CROE contain a detailed list of available cyber defences, but almost all of them are listed for illustrative purposes: (i) tools to establish network boundary (routers, firewalls, intrusion prevention systems, intrusion detection systems, virtual private network, demilitarised zone or proxies),[115] (ii) secure network protocols,[116] (iii) intrusion detection or prevention systems, end point security solutions[117] or, at the medium level of expectation, (iv) measures (such as network access control) to prevent unauthorised devices from connecting to the network.[118] A notable exception is encryption, which appears to be mandatory at the medium level (the words 'as a result of its data classification and risk assessment processes' do not imply a choice as to whether data should or should not be encrypted – on its face, this provision can only be read as allowing different types of encryption based on risk assessment).[119]

By comparison, the relevant provisions in the NYCRR 500 are significantly less detailed, but apply differently, depending on the defence instrument in question. While they do contain mandatory cyber defences, the CISO has the authority to implement alternatives. One example concerns access to data. On the one hand, the use of multi-factor identification – as a general protective measure against unauthorised access – is voluntary.[120] On the other hand, it must be used 'for any individual accessing the [firm's] internal networks from an external network'.[121] Yet, in the second case, the CISO is permitted to approve in writing the use of 'reasonably *equivalent* or *more secure* access controls'.[122] Another example relates to data encryption, which, as a general rule, is mandatory for non-public information held or

[115] CROE (n 59), s 2.3.2.1(10).

[116] ibid, s 2.3.2.1(14).

[117] ibid, s 2.3.2.1(16).

[118] ibid, s 2.3.2.1(24).

[119] See ibid, s 2.3.2.1(37).

[120] NYCCR (n 59), s 500.12(a).

[121] ibid, s 500.12(b).

[122] ibid.

transmitted by regulated entities.[123] Nonetheless, 'effective alternative compensating controls' are permissible if reviewed and approved by the CISO and subject to periodic (at least annual) review of both (i) the feasibility of encryption and (ii) effectiveness of the compensating controls.[124] The third example concerns a requirement to have in place 'policies and procedures for the secure disposal on a periodic basis' of certain non-public information 'that is no longer necessary for business operations or for other legitimate business purposes' (ie data cleanup).[125] Although data destruction is mandatory, the provision does not prescribe the frequency of each clean up, significantly watering down the potential effect of this rule (eg in case a firm decides to dispose of such data every 50 years). Interestingly, the CISO is not given an option to altogether disapply the measure in question: the latter is possible only when the law requires such information to be retained or where such disposal is 'not reasonably feasible due to the manner in which the information is maintained'.[126]

In contrast to the above examples, Russian regulators have developed more detailed substantive requirements targeting cyber defences. This is evidenced by the new regulations of the Bank of Russia (CBR) recently adopted as part of ongoing reforms with the aim of improving cybersecurity in the financial sector. Under CBR Instruction 3342-U, nationally important payment systems must ensure that (i) at least 25 per cent of their data protection software is developed in Russia,[127] and (ii) the cryptographic module of their payment cards is either locally certified by the Federal Security Service (FSS), or complies with security

[123] ibid, s 500.15(a).

[124] ibid, s 500.15(a)-(b).

[125] ibid, s 500.13.

[126] ibid.

[127] CBR Instruction 3342-U, s 1.1.

standards of at least two foreign payment systems.[128] Amendments to CBR Regulation 382-P coming into force in January 2020 set out not only a requirement of multifactor identification for money transfers, but also both mandatory and optional specifications of such identification (which nevertheless remain functional in nature and describe the expected functionality, but not specific technology used to achieve it).[129] Another set of amendments, in force from January 2024, imposes mandatory certification of hardware security modules and other cryptographic information protection facilities (CIPF) by the FSS.[130] Recently adopted Regulation 672-P targets the participants of the CBR's own payment system and requires, among other things, (i) (starting from July 2021) allocation of information infrastructure in separate computational networks and a minimum ('second') level of cybersecurity determined under the new national standard GOST R 57580.1-2017,[131] (ii) encryption of messages using FSS-certified CIPF and (iii) (starting from July 2021) encryption implementing mandatory two-way authentication and network- or link-level encryption.[132]

D. Recovery

The criticality of (*ex post*) recovery measures is determined by the 'assume breach' approach in modern cybersecurity theory: the question is not *whether* a firm's systems will be compromised, but *when*. Operational risk rules have routinely required implementation of business recovery measures, such as 'contingency and business continuity plans'.[133] Over time, these rules became more detailed, targeting cyber risks specifically, mostly via

[128] ibid, s 1.4.

[129] CBR Regulation 382-P, s 2.10.5-2.10.6 (effective from 01 January 2020).

[130] ibid, s 2.20 (effective from 01 January 2024).

[131] CBR Regulation 672-P, s 3-4 (effective 01 July 2021).

[132] ibid, s 14.2 (effective from 01 July 2021).

[133] Directive 2013/36/EU (n 43), Article 85(2).

obligations to set up data backup functionality. These provisions could be vague and abstract (such as an obligation to 'at least provide for the establishment of backup facilities')[134] or specific as to the measures taken and the time required to resume operations after breakdown (as is done in the SIPS Regulation, which requires (i) 'the use of a secondary site', (ii) resumption of critical system operations within two hours, (iii) capacity to settle all payments due by the end of the business day of disruption and (iv) annual testing and review of the continuity plan).[135]

Perhaps also as a result of their roots in general operational risk provisions, cybersecurity rules are almost surprisingly silent about measures required to ensure cyber efficiency of backup systems – which, if created replicating the design of the main system, are likely to replicate cyber vulnerabilities as well, thereby adding little (if anything) to the overall cybersecurity (if they can be breached in the same manner). In other words, implementation of a backup system following a cyberattack can be a lot trickier than following an earthquake – the latter (unlike the former) lacks the will to target the backup system as well.

E. Enforcement

Sanctions and possibility of enforcement are the key factors distinguishing 'soft law' and 'hard law'. That said, modern regulations that do set out bespoke cyber enforcement regimes, are faced with multiple challenges.

First, penalties for cybersecurity breaches under certain regulatory instruments may be non-existent or negligible, even in the context of EU regulations (ie rules with direct application in the Member States). For example, the eIDAS Regulation leaves sanctions for

[134] EMIR (n 62), Article 79(2).

[135] SIPS Regulation (n 53), Article 15.5.

Member States to decide. Member States, however, have been hesitant to develop meaningful sanctions for breaches under Article 19(1): for instance, in the UK the corresponding monetary penalty amounts to GBP 1,000 (reduced to GBP 800 if paid within 21 days).[136]

Second, some of the EU-wide rules lay down only the main enforcement principles, leaving the rest to national legislatures and regulators, creating opportunities for substantially different enforcement regimes for the same violations. Implementation of the NIS Directive is illustrative here. Whereas the directive itself requires penalties to be 'effective, proportionate and dissuasive',[137] the implementing regulations provide for a wide range of possible sanctions: up to GBP 17 million in the UK,[138] up to EUR 500,000 in Ireland[139] or only up to EUR 20,000 in Estonia.[140]

Third, the multiplicity of cybersecurity regulations creates the possibility of simultaneous enforcement under different instruments (eg under bespoke financial regulations and under the GDPR) for the same cyber incident. This fact has even been acknowledged in the UK regulations transposing the NIS Directive, which require the NIS enforcement authority to 'have regard to … whether the contravention is also liable to enforcement under another enactment'.[141]

Fourth, enforcement is complicated by specific features of cyber threats (in particular, the abovementioned 'assume breach' attitude). On the one hand, strict liability (eg in the form of penalties for permitting a cyber breach) appears unsuitable for an area where, depending

[136] UK Electronic Identification and Trust Services for Electronic Transactions Regulations 2016, Schedule 1, ss 2, 5.

[137] NIS Directive (n 29), Article 21.

[138] UK Network and Information Systems Regulations 2018, s 18(6)(d).

[139] Irish European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 (SI No 360 of 2018), s 34(b)(ii).

[140] Estonian Cybersecurity Act 2018, s 18(2).

[141] UK NIS Regulations 2018 (n 138), s 23(2)(e).

on the type of attacker, the target's ability to thwart an attack is not always determined by the target's own actions (eg in case of attackers – such as nation states – in possession of incomparable resources, cybersecurity intelligence and knowledge of undocumented features of cyber defences of the target). On the other hand, cyber regulations are predominantly principles-based and thus relevant authorities may have substantial discretion in 'translating' those principles into enforcement action (which must be specific). These factors, combined, preclude the adoption of clear and specific regulatory expectations easily verifiable *ex ante*. Consequently, it remains to be seen how the instruments providing for significant monetary sanctions for cybersecurity violations (eg the GDPR, Article 32) will be implemented in the context of financial services. In the context of the GDPR, although a number of investigations have already resulted in monetary penalties, at the time of writing there have been no major sanctions on financial firms imposed under Article 32. It is likely, however, that major investigations into alleged cybersecurity violations – in the form of poor security arrangements leading to a data breach – by British Airways[142] and Marriott International, Inc[143] (both under Article 32 GDPR) announced in July 2019 will provide certain guidance (even though they do not target financial firms).

V. PROSPECTS OF LEGAL HARMONISATION

Although the unique features of cyber threats have led to the development, over time, of bespoke cybersecurity regulation in finance, the resulting rules differ substantially, both within the EU and globally. Against this background, in December 2018 the Basel Committee on Banking Supervision (BCBS) issued a report which speculates:

[142] Information Commissioner's Office, 'Intention to Fine British Airways £183.39m Under GDPR for Data Breach' (08 July 2019) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-ico-announces-intention-to-fine-british-airways/>.

[143] Information Commissioner's Office,' Statement: Intention to fine Marriott International, Inc More than £99 Million Under GDPR for Data Breach (09 July 2019) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/>.

> Banks and supervisory authorities may benefit from harmonisation and standardisation, not just of supervisory expectations, but also of the information requested by supervisors and the tools used to collect it.[144]

It is hard to argue with this very cautious supposition, at least for three reasons.

First, harmonisation is necessary to deal with existing (and potential) overlaps in cybersecurity regulation. Multiplicity of regulations, particularly when they are developed independently of each other, always brings with it risks of collisions. Although it is clear from section III above that the patchwork of cybersecurity rules in the EU is a prime example of a regulatory framework capable of generating legal conflicts, the problem is definitely not unique. For instance, the ongoing modernisation of Russia's cybersecurity framework in finance was preceded by a request of the Association of Russian Banks (ARB), addressed to the CBR, to develop a common development strategy for information security of credit institutions. The head of the ARB explained that, at the time, responsibilities of information security personnel were regulated, by over 130 documents, including, inter alia, 50 federal laws, 20 presidential and government decrees, 15 acts adopted by federal ministries and agencies, as well as 25 regulations of the CBR.[145] Needless to say, on a transnational basis (as in the EU), the possibility of overlaps is likely to be higher.

Actual sources of conflicts differ, but can be generally allocated to one of three categories:

1. Inconsistent terminology, such as lack of a common approach in EU rules concerning the legal status of cybersecurity risks: some instruments do not separate cybersecurity risks

[144] Basel Committee on Banking Supervision (n 84) 9.

[145] S Fadeichev, 'Банкиры просят ЦБ создать единую стратегию развития информационной безопасности' ('Bankers Ask the CB to Create a Common Development Strategy for Information Security') (14 February 2017) <https://tass.ru/ekonomika/4020544>.

from operational risks,[146] while others expressly refer to 'operational *and security* risks'.[147] A related issue concerns lack of clear differentiation between cybersecurity risks and general IT risks.

2. Overlapping requirements in sectoral (eg ECB regulations) and cross-sectoral instruments (eg NIS Directive, GDPR). While a degree of similarity of regulatory regimes is not an issue per se (such as in the case commonly observed requirements to implement appropriate cybersecurity measures), different reporting or penetration testing regimes multiply compliance obligations. Although some instruments attempt to address overlaps, such examples are rare and raise challenges of their own. For example, the NIS Directive, in theory, allows alternative sector-specific requirements to take priority, provided that the latter are 'at least equivalent in effect' (Article 1(7)) – yet comparing the two sets of rules (and assessing 'equivalence') may be difficult, such as when one set of requirements is more comprehensive in some aspects, but is less demanding in others.

3. Overlapping requirements in local and federal (or national and supranational) instruments. For example, in the US cyber-events must be notified to the regulators under state cyber-resilience frameworks, such as the NYCRR 500,[148] as well as in suspicious activity reports for the US Financial Crimes Enforcement Network (FinCEN).[149] Furthermore, although this article is not based on an exhaustive analysis of EU Member State cybersecurity regulations (and, therefore, additional research is required in this respect), one can assume that there is scope for similar legal conflicts in the EU as well.

[146] Directive 2013/36/EU (n 43), Article 85(1).

[147] PSD2 (n 46), Article 95(1) (emphasis added).

[148] NYCCR 500, s 500.17.

[149] FinCEN, 'Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime' (25 October 2016) <https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf>.

Second, an international response is needed to address the cross-border nature of cyber threats, which, as noted in the EU FinTech Action Plan, 'requires a high degree of alignment of national regulatory and supervisory requirements and expectations'.[150]

Third, harmonisation can provide useful guidance for legislatures and regulators lacking cybersecurity expertise, while also serving as evidence of readiness of participating jurisdictions to unify their cyber practices (which requires considerably more effort compared to various forms of non-binding international guidance) and convince others to follow their example. In the author's experience, there is a considerable dearth in cybersecurity expertise among certain regulators, particularly in the developing world.

Before discussing the scope of possible harmonisation (ie '*what* to harmonise'), let us first briefly consider the toolset available to legislators and regulators (ie '*how* to harmonise').

A. Emerging International Guidance

With regulators' radars turning towards cybersecurity, the emergence of international guidance in this area was perhaps only a matter of time. At the time of writing, however, such guidance for the financial sector is still in the early, exploratory stages, largely focusing on high level issues and review of reported practices. Examples include various 'fundamental elements' publications issued by the G7,[151] overview of international cybersecurity practices

[150] European Commission (n 82) 15.

[151] See G7 (n 99); G7, 'G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector' (2017) <https://www.bundesbank.de/resource/blob/665510/3a6628d69698bf3bb04bf94629f0ac84/mL/2017-10-26-g7-fe-for-effective-assessment-data.pdf>; G7, 'Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector' (2018) <https://www.bundesbank.de/resource/blob/764692/01503c2cb8a58e44a862bee170d34545/mL/2018-10-24-g-7-fundamental-elements-for-third-party-cyber-risk-data.pdf>; G7, 'Fundamental Elements for Threat-Led Penetration Testing' (2018) <https://www.bundesbank.de/resource/blob/764690/792725ab3e779617a2fe28a03c303940/mL/2018-10-24-g-7-fundamental-elements-for-threat-led-penetration-testing-data.pdf>.

by the BCBS,[152] OECD recommendations,[153] various publications by the FSB,[154] IAIS,[155] World Bank Group,[156] IMF[157] or CPMI and IOSCO.[158] The guidelines published by the latter two organisations in 2016 require financial market infrastructures to 'immediately take necessary steps … to improve their cyber resilience'[159] and have paved the way for legal (domestic and international) reforms, such as revision of Regulation 795/2014 by the ECB in 2017[160] or the CROE (intended to operationalise the guidelines).[161]

B. Technical Standards and Industry Self-regulation

Instead of reinventing the wheel, regulators and legislators frequently rely on existing technical standards as a basis for cybersecurity rules and frameworks.[162] The key technical

[152] BCBS (n 84).

[153] Organisation for Economic Co-operation and Development (OECD), 'OECD Recommendation of the Council on the Protection of Critical Information Infrastructures' (2008) <https://www.oecd.org/sti/40825404.pdf>. The document is being revised in 2019. See also OECD, 'Digital Security Risk Management for Economic and Social Prosperity' (2015) <https://read.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en#page1>.

[154] See, eg, Financial Stability Board, 'Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices' (2017) <https://www.fsb.org/wp-content/uploads/P131017-2.pdf>; Financial Stability Board, 'Cyber Lexicon' (2018) (n 10).

[155] International Association of Insurance Supervisors (IAIS), 'Issues Paper on Cyber Risk to the Insurance Sector' (2016) <https://www.iaisweb.org/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector>; IAIS, 'Application Paper on Supervision of Insurer Cybersecurity' (2018) <https://www.iaisweb.org/file/77763/application-paper-on-supervision-of-insurer-cybersecurity>.

[156] World Bank Group, 'Financial Sector's Cybersecurity: Regulations and Supervision' (2018) <http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf>.

[157] A Bouveret (n 19). The publication is part of IMF research, but may not necessarily represent the views of the IMF.

[158] BIS Committee on Payments and Market Infrastructures and International Organisation of Securities Commissions (n 15).

[159] ibid 3.

[160] See ECB (n 57), Preamble, para 1.

[161] CROE (n 59), 3.

[162] See Annex A in FSB (n 154) 44.

cybersecurity standards have been developed by the ISO and IEC,[163] NIST,[164] ISACA,[165] CIS,[166] ISF[167] and FFIEC[168] – and, just like the international guidance mentioned in the previous section, can be used to develop a harmonised approach to cybersecurity in the financial sector. Indeed, some of the recent regulatory instruments have taken advantage of the existing standards. In the EU, the CROE were developed by the ECB using 'as basis' not one, but multiple standards (namely, the NIST Cybersecurity Framework, ISO/IEC 27002, COBIT 5, the ISF's Standard of Good Practice for Information Security and the FFIEC Cybersecurity Assessment Tool).[169] In the US, FinCEN uses NIST terminology, namely 'the Glossary of Key Information Security Terms and other publications … for definitions of cyber-related terms'.[170]

Although the advantages of using established technical standards are clear, several points should be considered by rule makers.

First, cybersecurity rules should clearly and unambiguously state whether the use of technical standards is (i) required, (ii) encouraged, or (iii) merely possible. In the EU, all three options have been implemented in different instruments. Consider the following three examples. According to Regulation 153/2013, a CCP '*shall base* its information technology

[163] International Organization for Standardization and International Electrotechnical Commission, 'ISO/IEC 27000 Family - Information Security Management Systems' <https://www.iso.org/isoiec-27001-information-security.html>.

[164] National Institute of Standards and Technology, 'Cybersecurity Framework' <https://www.nist.gov/cyberframework>.

[165] Information Systems Audit and Control Association, 'COBIT 5 Framework' <http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx>.

[166] Center for Internet Security, 'CIS Controls' <https://www.cisecurity.org/controls/>.

[167] Information Security Forum, 'The ISF Standard of Good Practice for Information Security 2018' https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/>.

[168] Federal Financial Institutions Examination Council, 'Cybersecurity Assessment Tool' (2017) <https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf>.

[169] CROE (n 59) 3.

[170] FinCEN (n 149) 2.

systems on internationally recognised technical standards'.[171] In contrast, under the NIS Directive, Member States must '*encourage* the use of European or internationally accepted standards and specifications relevant to the security of network and information systems'.[172] Finally, in the CROE the ECB uses multiple approaches. On the one hand, an FMI is required to use various standards '*as a benchmark* for designing its cyber resilience framework' (and thus the use of standards is clearly encouraged, but not mandated).[173] On the other hand, an FMI's information security management system '*could be based* on a combination of well-recognised international standards'[174] (implying that this is merely one of available options, but not even the preferred one).[175]

Second, abstract references to 'recognised' or 'accepted' standards generate uncertainty when their use is mandatory (and failure to apply them can be sanctioned). For example, the above-mentioned obligation to use 'internationally recognised technical standards' in Regulation 153/2013 (Article 9(2)) raises questions of interpretation. How does one determine which technical standards have been recognised 'internationally'? What if a standard developed in one country is used abroad, but only in a handful of other jurisdictions? If other European rules are of any relevance, the NIS Directive suggests that an international level of acceptance is a higher standard than regional (since Article 19(1) clearly distinguishes between 'European' and 'internationally accepted' standards).

Third, incorporation of industry-driven technical standards into cybersecurity rules sends a co-regulatory message to the industry and creates the risk of regulatory capture. It should be noted that regulators have no control over third-party issued standards, which could

[171] Regulation 153/2013 (n 64), Article 9(2) (emphasis added).

[172] NIS Directive (n 29), Article 19(1) (emphasis added).

[173] CROE (n 59), s 2.1.2.1(8) (emphasis added).

[174] ibid, s 2.3.2.1(6) (emphasis added).

[175] See also ibid, s 2.3.2.1(33).

be revised in an undesirable fashion or even lag behind best practices (although the latter issue is likely to be relevant only for regulators adopting cutting edge solutions). The complexity of building adequate cybersecurity rules is undeniable but should not be overestimated: industry guidance cannot replace regulation. We have already seen this challenge in the field of so-called artificial intelligence (AI), where technology firms have been actively lobbying for self-regulation of AI.[176] It should then come as no surprise when the industry argues that cyber risks evolve too fast to be properly regulated. The issue is definitely not new, but regulators should be aware of the underlying implications.

C. Mode of Harmonisation

Harmonisation of cybersecurity regulations can take the form of soft law (informal guidance, recommendations, summaries of practices) or hard law (supranational regulation, international conventions), or both.[177] While soft law options are always open for regulators, their effectiveness in reaching a common cybersecurity standard is understandably limited. Yet, the feasibility of a hard law approach is largely based on the scope of the projected action: harmonisation of key principles or substantive rules. So far, cybersecurity instruments in the EU have largely followed the principles-based approach (see section IV). Individual Member States have also expressed support for this method. For example, the UK's recently established National Cyber Security Centre explains in its NIS guidance that a principles-

[176] See, eg, T Greene, 'US Government is Clueless About AI and Shouldn't be Allowed to Regulate It' (25 October 2017) <https://thenextweb.com/artificial-intelligence/2017/10/24/us-government-is-clueless-about-ai-and-shouldnt-be-allowed-to-regulate-it/>.

[177] As noted earlier, for the purposes of this article, 'regulation' does not include informal measures (such as industry self-regulation). See n 14.

based approach is preferable, since 'it is *not possible* to devise an effective set of prescriptive rules for good cyber security'.[178]

In the light of the above, it is conceivable that harmonised principles-based provisions (particularly if they focus on cyber governance) are likely to be more readily accepted by multiple regulators if integrated into hard international law. Another (alternative or follow-up) option would be to pursue staggered harmonisation, starting with a *de minimis* substantive harmonisation, ie an agreement on a set of common baseline substantive provisions, the importance and implications of which are discussed in the next section.

VI. SCOPE OF LEGAL HARMONISATION

This section focuses on the scope of future harmonisation of cybersecurity rules in finance in the light of two related challenges: (i) establishing a *de minimis* set of common requirements and (ii) harmonisation beyond the minimum level.

A. Establishing a Baseline

The importance of setting up a certain cybersecurity baseline was captured well in section 500.00 of the NYCRR 500, which notes that 'certain regulatory minimum standards are warranted, while not being overly prescriptive'. However, in the harmonisation context, the task of determining a common denominator gets noticeably more complicated, and not only because multiple regulators are involved. Minimum standards and harmonised guidance are particularly important today due to the rapid evolution of the financial services landscape caused by small financial technology (FinTech) firms (often start-ups) entering the financial market. These small firms are likely to lack the expertise and resources to decipher the high-

[178] National Cyber Security Centre, 'NCSC NIS Guidance' (15 November 2018) <https://www.ncsc.gov.uk/collection/nis-directive?curPage=/collection/nis-directive/introduction-to-the-nis-directive>.

level abstract requirements to have 'appropriate' cybersecurity in place or to navigate and implement the relevant technical standards.

Let us now consider what factors should be considered when determining the scope of the 'baseline' harmonised cybersecurity regulations for finance.

First, whereas multiple jurisdictions have already adopted national cybersecurity strategies,[179] cybersecurity in finance – generally accepted as one of the key sectors from the cyber perspective – is often regulated without a dedicated *sector-wide strategy*, generating overlaps.

Second, efficient cybersecurity regulation (in particular during subsequent review and modification of existing rules) requires access to reliable statistical data. To generate sufficient amounts of data, cybersecurity reporting regimes concerning cyber events need to be put in place as early as possible (thus, ideally, they are needed as part of *de minimis* harmonisation). However, since numerous, and often conflicting, cyber reporting requirements have already been established in multiple legal instruments, a harmonised regime will need to take into account the following:

1. Efficient reporting regimes should cover a broad spectrum of entities to minimise freeriding opportunities thus disincentivising 'under the radar' attitude.

[179] See, eg, European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (n 21); Cyber Security Agency of Singapore, 'Singapore's Cybersecurity Strategy' (2016) <https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf>; Australian Government, 'Australia's Cyber Security Strategy' (2016) <https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf>; President of the United States of America, 'National Cyber Strategy of the United States of America' (2018) <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>. See also the obligation to 'adopt a national strategy on the security of network and information systems' in Article 7(1) of the NIS Directive (n 29) and the national strategies across the EU developed in response to this requirement: European Commission, 'State-of-play of the Transposition of the NIS Directive' (2018) <https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive>.

2. Reporting every single cyber event may be problematic, and thus a materiality criterion (or criteria) should be introduced, at least initially. However, abstract and unclear materiality criteria should be avoided to reduce uncertainty.

3. Although reporting can be to different entities (including regulators, peer financial firms and clients), the *de minimis* regime should at least incorporate reporting to regulators (which can be done on a confidential basis). Information sharing obligations can be introduced separately (see section VI(B)(4) below).

4. A single basic reporting format and standardised requirements should promote efficiency.

5. Timing of *ex post* (after the fact) notices of cyber events should take into account existing practices, which, inter alia, include the following standards:

    - 'without undue delay' not qualified by additional requirements;[180]
    - 'without undue delay' qualified by additional requirements;[181]
    - 'as soon as practicable';[182]
    - within 24 hours;[183]
    - within 1 business day;[184]

[180] PSD2 (n 46), Article 96(1); NIS Directive (n 29), Articles 14(3) and 16(3); eIDAS Regulation (n 39), Article 19(2) (reporting to clients).

[181] GDPR (n 35), Article 33. Notification must be made, where feasible, within 72 hours of becoming aware of it. If the controller fails to give notice within 72 hours, it must explain the reasons for the delay.

[182] Australia's Privacy Act 1988, s 26WK.

[183] eIDAS Regulation (n 39), Article 19(2) (reporting to regulators).

- within 72 hours;[185]

- two-tier reporting: (i) initial (within 2 hours) and (ii) subsequent (within 14 days after the initial report);[186]

- three-tier reporting: (i) initial (within 4 hours), (ii) intermediate (within 3 business days thereafter) and (iii) final (within 2 weeks after business is deemed back to normal);[187]

- three-tier reporting: (i) initial (within 3 hours), (ii) intermediate (within 3 hours, although the author notes this might be a textual omission in the text of the instrument) and (iii) final (within 3 business days after closure of the cyber incident);[188]

- three-tier reporting: (i) initial (within 24 hours), (ii) intermediate (within 2 business days thereafter) and (iii) final (within 3 business days after closure of the cyber incident);[189]

- not later than 1 business day prior to any 'incident disclosures related to violations of information security obligations … including posting on official websites, issuing press-releases and holding press-conferences;[190]

---

[184] See Annex 1 to the Order 321 of 25 June 2018 of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation, s 9(1).

[185] NYCRR 500, s 500.17(a).

[186] Singapore Cybersecurity Act 2018, s 14; Singapore Cybersecurity (Critical Information Infrastructure) Regulations 2018, s 5.

[187] EBA Guidelines on Major Incident Reporting (n 50), ss 2.7-2.21.

[188] Russian CBR Standard STO BR BFBO-1.5-2018 Security of Financial (Banking) Operations: Management of Information Security Incidents (2018), s 6 (for important entities in the critical information infrastructure only).

[189] ibid.

- reports covering a calendar period (eg the preceding calendar year).[191]

Third, the unique characteristics of cyber threats (see section II above) imply that cybersecurity regulations may get outdated quickly and thus require periodic review even at the baseline level of harmonisation. This aspect complicates the prospects of hard international law (ie a treaty) but does not disqualify it. After all, the need to amend the scope of an international convention is a recurring challenge, and lessons can be learned from existing treaties.[192]

Fourth, in designing the minimum level of cybersecurity expectations at the baseline harmonisation level, rule makers should consider whether the lowest common denominator (reflecting the minimum pre-existing level of cybersecurity) is sufficient or whether a *higher minimum* level should be targeted, in the light of increasing interconnectedness of the financial sector – and consider providing additional tools to assist the regulated entities. This is particularly important for smaller FinTech firms and even banks (in countries with an unconsolidated banking sector and a large number of credit institutions) that may lack the resources or sophistication to comply with all the requirements on their own. Common cybersecurity resources can be developed to assist businesses with lower levels of cyber-preparedness. These may include setting up a purpose-built outsourcing entity controlled by the regulator – an initiative considered in February 2019 by the Russian authorities. On the

---

[190] CBR Regulation 382-P, s 2.13.1. See also CBR Regulation 683-P, s 8; CBR Regulation 684-P, s 15.

[191] NYCRR 500, s 500.17(b).

[192] A notable example is the MAC Protocol to the 2001 Convention on International Interests in Mobile Equipment developed by UNIDROIT and adopted at a Diplomatic Conference in Pretoria in November 2019. The treaty has to deal with periodic changes to its scope as a result of revision of the Harmonised Commodity Description and Coding System developed by the World Customs Organization that is used to determine the types of assets to which the MAC Protocol applies. For more detail see T Rodríguez de las Heras Ballell and M Hara, 'MAC Protocol and Treaty Design: Examination of the Delimitation of Scope and Mechanism of Amendment' (2017) 6 Cape Town Convention Journal 10.

one hand, the regulators in the country with almost 150 small banks with a 'basic' (ie limited) license were concerned that engagement of established outsourcing cybersecurity companies may be too costly for smaller firms, which are likely to get captured in specific digital architecture and then slammed with high tariffs.[193] At the same time, it was acknowledged that financial institutions were unlikely to entrust cybersecurity to specialised firms established by competitors, which led to the concept of a regulator-controlled outsourcing entity. Nonetheless, one should consider the risks of such proposal, including the cost of outsourcing in question. In countries with a limited pool of cybersecurity talent, a newly established specialised entity is likely to be staffed by experts poached from competitors, driving the overall price of outsourcing services up (although in a harmonised (international) setting the competition implications may not be as pronounced).

B. Beyond the Baseline

Once the baseline level of cybersecurity requirements is established, one should consider expanding the scope of the regulatory regime to promote a higher overall level of cyber standards and practices. At the time of writing, higher standards have been devised only for a limited number of businesses, such as FMIs (see the CROE), and thus it is likely that any harmonisation of cybersecurity rules at the baseline level will coexist with, or follow, an expansion of higher level expectations to other financial firms, such as large banks.

There are different approaches to setting up more comprehensive cybersecurity requirements, most notably in the form of multi-tier frameworks. The CROE, for example, set out three levels of expectation: (i) 'evolving', (ii) 'advancing' and (iii) 'innovating'. Different levels of cyber maturity are expected from different payment systems: prominently

[193] V Goryacheva, K Zhukova and V Soldatskikh, 'Кибербезопасность ушла на базу' ('Cybersecurity Has Gone to the Base') (Kommersant, 19 February 2019) <https://www.kommersant.ru/doc/3888889>.

important retail payment systems (PIRPS) and other retail payment systems (ORPS) are to achieve the lower, 'evolving' level, whereas systemically important payment systems (SIPS) (alongside T2S) are expected to meet the higher 'advancing' level of expectation.[194] All entities are expected to 'take active steps' to reach the next level.[195]

In contrast, the Russian government established several multi-tier cybersecurity frameworks:

- one for processors of personal data (ie personal data operators or third parties engaged by them);
- one specifically for credit institutions; and
- one specifically for non-credit financial institutions.

The former is a four-tier framework, with four different levels of requirements relating to security of personal data. Tier allocation is based on a combination of three criteria: (i) types of threats faced by the information system, (ii) types of data stored (publicly available, biometric, special – eg data on health, race, nationality etc – or any other data), (iii) number of personal data subjects whose data are stored (the threshold parameter is 100,000 data subjects) and (iv) categories of personal data subjects concerned (employees of the operator or any other data subjects).[196] The types of threats are classified based on whether there exist (a) no threats related to undocumented features (level three threats), (b) threats related to undocumented features in application software (level two threats) or (c) threats related to undocumented features in system software (level one threats). The four levels of security

[194] CROE (n 59), s 1.4.2.

[195] ibid.

[196] Russian Government Regulation 1119 of 01 November 2012 'On Establishing the Requirements for Protection of Personal Data Processed in Personal Data Information Systems', s 9-12.

requirements are structured as a pyramid, in which each level above the lowest (fourth) level incorporates all the security measures in all of the lower levels, as explained below.

- Fourth (lowest) level requirements include: (i) limitation of access to premises hosting the information system in question, (ii) security of data storage devices, (iii) drawing up a list of authorised users of data and (iv) using appropriate data security instruments.[197]

- Third level requirements also include appointment of an employee responsible for the security of personal data.[198]

- Second level requirements add restrictions on access to the electronic message log.[199]

- First (highest) level requirements further add (i) automatic logging of any changes of access permissions and (ii) setting up an internal division responsible for the security of personal data or making one of the existing divisions responsible for the security of personal data.[200]

The second Russian multi-tier framework focuses on cybersecurity among credit institutions and is based on a combination of two new instruments: CBR Regulation 683-P[201] issued in April 2019 and a corresponding national cybersecurity standard for financial institutions.[202] The latter establishes three levels of information protection (from lowest to

[197] ibid, s 13.

[198] ibid, s 14.

[199] ibid, s 15.

[200] ibid, s 16.

[201] CBR Regulation 683-P of 17 April 2019 'On Mandatory Requirements for Credit Institutions Concerning Security of Information in the Course of Banking Activities to Combat Money Transfer without Client Consent'.

[202] GOST R 57580.1-2017 'Security of Financial (Banking) Operations. Information Protection of Financial Organizations. Basic set of Organizational and Technical Measures' (2017).

highest): (i) 'minimal', (ii) 'standard' and (iii) 'enhanced'.[203] Pursuant to CBR Regulation 683-P, starting from 01 January 2021, all credit institutions will be required to comply either with the 'standard', or with the 'enhanced' level requirements, depending on their type:

1. the highest ('enhanced') level requirements apply to three groups of credit institutions: (a) systemically important credit institutions, (b) credit institutions acting as payment infrastructure operators of systemically important payment systems and (c) credit institutions that are important for the payment services market; and

2. the medium ('standard') level requirements apply to all other credit institutions.[204]

The third Russian framework was also established in April 2019, by virtue of CBR Regulation 684-P.[205] It relies on the same national cybersecurity standard (GOST R 57580.1-2017) and similarly requires non-credit financial institutions to comply either with the 'standard', or with the 'enhanced' level requirements:

1. the highest ('enhanced') level requirements apply to two groups of non-credit institutions: (a) central counterparties and (b) central depository; and

2. the medium ('standard') level requirements apply to (a) specialised depositories of investment and non-state pension funds, (b) clearing organisations, (c) market operators, (d) major insurance organisations, (e) certain non-state pension funds, (f) repositories, (g)

[203] ibid, s 6.7. The three levels are associated with different sets of requirements relating to (i) data protection system (access control, network security, control of integrity and security of information infrastructure, protection against malicious code, prevention of information leaks, information security incident management, virtualisation security and information security of remote access using mobile devices), (ii) organisation and management of data protection and (iii) data protection in automated systems and applications.

[204] CBR Regulation 683-P, 3.1 (effective from 01 January 2021).

[205] CBR Regulation 684-P of 17 April 2019 'On Mandatory Requirements for Non-Credit Financial Institutions Concerning Security of Information in the Course of Financial Market Activities to Combat Unlawful Financial Operations'.

major brokers and dealers, (h) major depositories, (i) major registrators and (j) major investment managers.[206]

Another key factor that needs to be considered in designing higher level requirements is the risk associated with data-intensive businesses (sometimes referred to as 'TechFins')[207] entering the financial services market. The upcoming launch of a new digital currency 'Libra'[208] is one example of such transition. Although data-driven businesses can be expected to have certain cybersecurity measures in place (eg in relation to personal data protection), the latter are likely to be insufficient compared to the requirements applicable in the financial sector – yet the scale of some of these businesses is likely to make evaluation of their compliance extremely difficult once they enter the financial market. To soften the transition, regulators may consider cross-sectoral cybersecurity harmonisation to ensure that major data firms and financial institutions are subject to similar cybersecurity requirements.

This section will now consider some of the key additional provisions identified in existing cybersecurity regulations and the corresponding implications.

1. Keeping regulations up to date

Although bespoke cybersecurity regulations are still in their infancy, some of the existing rules, particularly in the EU, incorporate references to best practices and latest technological developments in the context of designing cybersecurity frameworks. These come in different forms and can broadly be allocated to one of two groups.

[206] ibid, s 5 (effective from 01 January 2021).

[207] See D Zetzsche, R Buckley and D Arner, 'From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance' (2018) 14 New York University Journal of Law and Business 393.

[208] See Libra, 'An Introduction to Libra' (2019) <https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US-1.pdf>.

The first group contains provisions considering the current level of technology. For example, under the GDPR, technical and organisational measures to ensure security of data processing must be implemented 'taking into account the state of the art'.[209] Similar provisions can be found in the NIS Directive, which calls for cybersecurity measures to be designed 'having regard to the state of the art' – a requirement that applies to operators of essential services and digital service providers.[210] A similar provision in the eIDAS Regulation uses a different language ('having regard to the latest technological developments'), albeit seemingly with little change in meaning. In contrast to the above examples, the CROE make the use of 'state-of-the art [*sic*] threat detection' mandatory at the highest ('innovating') level of expectation.[211] In addition, at the same level, FMIs are also expected to 'explore potential technologies to constantly adjust and refine … security countermeasures'.[212]

The second group implements provisions focused on current best practices. The CROE expect FMIs to 'employ best practices when implementing changes' at the basic ('evolving') level[213] – and to set up change management process based on 'well-established and industry-recognised standards and best practices' at the 'advancing' level.[214] In the context of cybersecurity testing (at the 'advancing' level), FMIs are also expected to 'adopt best practices' to fix identified weaknesses.[215] Regulation 153/2013 goes further and requires each

[209] GDPR (n 38), Article 32(1).

[210] NIS Directive (n 29), Articles 14(1) and 16(1).

[211] CROE (n 59), s 2.4.2(21).

[212] ibid, s 2.3.2.1(9).

[213] ibid, s 2.3.2.1(44).

[214] ibid, s 2.3.2.1(52).

[215] ibid, s 2.6.2(23).

CCP to 'base its information technology systems on … industry best practices' (although it does not explain to what extent those practices need to be implemented).[216]

Both groups have two things in common. First, they aim to facilitate the highest possible (at the time) level of preparedness. Second, the relevant provisions deliberately use discreet language, generally encouraging the use of up-to-date techniques, but not always making them mandatory. Yet, the scope of the two standards differs substantially, even though both can be seen as objective in nature. The first group is concerned with the level of technology –ie what is physically possible at the time. The second group is more reactive, as it is based on the current level of industry practices, which may or may not adequately tackle cybersecurity issues at the current level of technology. Consequently, the former group is likely targeted at the more sophisticated firms having sufficient resources to analyse the level of technological advancement in the entire sector. Perhaps, for this reason, in the CROE the state-of-the-art requirements can be found in provisions relating to the highest ('innovating') level of expectation, whereas the lower levels target best practices.

For obvious reasons, international harmonisation requiring implementation of state-of-the-art technology or best practices is a serious challenge and is unlikely to be pursued at an early stage. Nevertheless, regulators should consider existing international lawmaking experience. One of the most relevant (and, most importantly, working) examples is Article 28 of the 2001 Convention on International Interests in Mobile Equipment (CTC). The CTC is a treaty establishing an international regime for secured financing transactions over mobile equipment (such as airframes, aircraft engines, helicopters, railway rolling stock and space assets). An important element of this regime is an International Registry used to record interests of financing parties and thereby establishing priorities. The International Registry is

[216] Regulation 153/2013 (n 64), Article 9(2).

maintained by a Registrar – an organisation which must 'ensure [its] efficient operation'.[217] To give comfort to financing parties and encourage registrations in the International Registry (which has now become the global de facto standard in international aviation financing), the Registrar is subject to unlimited liability for its own errors or omissions, as well as for any 'malfunction of the international registration system' (including cybersecurity breaches). The Registrar may escape liability only where the malfunction is caused 'by an event of an inevitable and irresistible nature, which could not be prevented by using the *best practices* in current use in the field of electronic registry design and operation, including those related to back-up and *systems security* and networking'.[218] Such a high level of liability requires the Registrar to perform periodic review of registry best practices, but, most importantly, demonstrates that the highest levels of cybersecurity can already be found in international conventions – and not just as recommendations, but in the form of enforceable mandatory provisions.

The obvious challenge of the CTC approach, as well as any of the provisions found in the two groups mentioned above, is the lack of certainty – particularly in the context of non-compliance and enforcement.[219]

2. Penetration testing

Penetration testing (in particular threat-led penetration testing or 'TLPT') is recognised as 'the most advanced tool for cyber resilience testing',[220] as well as one of the most useful tools to measure the existing level of preparedness in the area of cybersecurity. Whereas

[217] CTC, Article 17(5).

[218] ibid, Article 28(1) (emphasis added).

[219] See section IV(E) above.

[220] Joint Committee of the European Supervisory Authorities, 'Joint Advice of the European Supervisory Authorities' JC 2019 25 (10 April 2019) 10 <https://eba.europa.eu/documents/10180/2551996/JC+2019+25+%28Joint+ESAs+Advice+on+a+coherent+cyber+resilience+testing+framework%29.pdf>.

cybersecurity testing (a much broader concept) is a common mandatory requirement of regulatory frameworks around the globe, TLPT in finance has not reached that stage yet.

In the EU, application of the TIBER-EU framework remains at the discretion of the relevant (European or national) authorities and, at the time of writing, it has not been widely adopted as a mandatory standard.[221] In contrast, the CROE do contain certain penetration testing requirements, but their scope varies depending on the level of regulatory expectation: the lowest ('evolving') level merely requires penetration tests to be conducted at least annually engaging all critical external and internal stakeholders, whereas at the middle ('advancing') level such testing must 'simulate realistic attack techniques' and be accompanied by red team[222] exercises to test critical functions for vulnerabilities using 'reliable and valuable cyber threat intelligence'.[223] The relevant red team tests are expected to be conducted by expert third parties, since '*internal* red team capability' is required only at the highest, 'innovating' level[224] (which, as noted previously,[225] is not mandatory even for entities over which the Eurosystem has competence). Other sectoral regulations (eg those applicable to investment firms engaged in algorithmic trading) are not as specific and merely require penetration testing to take place periodically, eg on an annual basis.[226]

Outside the EU, penetration testing is gaining popularity in the financial sector, but the practice has not been implemented uniformly. In Singapore, despite the existence of a

[221] See n 37.

[222] 'Red team testing' is synonymous to 'threat-led penetration testing' and is defined by the FSB as 'a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors' that is 'based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations'. See Financial Stability Board, 'Cyber Lexicon' (n 10) 13.

[223] CROE (n 59), ss 2.6.2(19)-2.6.2(20); 2.6.2(28)-2.6.2(30).

[224] ibid, s 2.6.2(42) (emphasis added).

[225] See n 194.

[226] Regulation (EU) 2017/589 (n 79), Article 18(4).

dedicated guidelines,[227] it remains voluntary – although regulators may conduct 'cybersecurity exercises' to test the readiness of owners of critical information infrastructure to respond to major cybersecurity incidents (in which case participation becomes mandatory, with non-compliance punishable by a monetary penalty up to SGD 100,000).[228] While the scope of a 'cybersecurity exercise' is not defined in the Cybersecurity Act 2018, it may, on its face, include penetration testing.

Under the NYCRR 500, penetration testing is mandatory, on an annual basis, but the requirement only applies absent effective continuous monitoring vulnerability-detection systems.[229]

In Hong Kong, penetration testing (known as 'iCAST' – Intelligence-led Cyber Attack Simulation Testing) has recently been rolled out within the banking sector as part of the Cybersecurity Fortification Initiative. Strictly speaking, iCAST is not an industry-wide exercise: it is preceded by an assessment of inherent cybersecurity risks (categorised as 'low', 'medium' or 'high') and becomes mandatory only for authorised institutions with 'medium' and 'high' risk levels.[230] The iCAST testing was conducted in three phases: the first one, due by June 2018, included 30 institutions (all major retail banks, selected global banks and several smaller firms);[231] the second one was due by September 2019 and included 60

[227] See The Association of Banks of Singapore, 'Penetration Testing Guidelines For the Financial Industry in Singapore' (2015) <https://abs.org.sg/docs/library/abs-pen-test-guidelines.pdf>. In 2018, another guidance was released – see The Association of Banks of Singapore, 'Red Team: Adversarial Attack Simulation Exercises; Guidelines for the Financial Industry in Singapore' (2018) <https://abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines-v1-06766a69f299c69658b7dff00006ed795.pdf>.

[228] Singapore Cybersecurity Act 2018, s 16.

[229] NYCRR 500, s 500.05.

[230] Hong Kong Monetary Authority, 'Cybersecurity Fortification Initiative' (21 December 2016) 1 <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf>.

[231] ibid 2.

institutions; and the third one is expected to be finalised by mid-2020 and will cover the remaining (around 90) authorised institutions.[232]

Under Russian law, penetration testing is also mandatory for selected financial institutions. These include (i) money transfer operators and payment infrastructure operators (required to conduct annual tests),[233] (ii) credit institutions (also required to conduct annual tests)[234] and (iii) non-credit financial institutions subject to the 'standard' or 'enhanced' levels of cyber resilience[235] (no time frame is given, and the obligation comes into force in January 2021).[236]

So far, harmonisation of threat-led penetration testing regimes (ie red teaming) has only just started but remains a complex task, given that the above practices are not yet widely adopted internationally and also bearing in mind that regulators tend to hasten slowly (with cross-border regulatory exercises being particularly difficult). Nonetheless, the work of the G7[237] and frameworks like TIBER-EU, which push for international harmonisation, shed a tiny ray of hope.

Furthermore, regulators will have to take into account the different level of preparedness in different jurisdictions, as recently stressed by the European Supervisory Authorities arguing that, in their view, 'it would be premature to pursue a specific cyber

[232] Hong Kong Monetary Authority, 'Implementation of Cyber Resilience Assessment Framework' (12 June 2018) 1-2 <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf>.

[233] CBR Regulation 382-P, s 2.5.5.1.

[234] CBR Regulation 683-P, s 3.2.

[235] See n 206 and the corresponding discussion.

[236] CBR Regulation 684-P, s 5.4 (effective from 01 January 2021).

[237] See G7, 'G7 Fundamental Elements for Threat-led Penetration Testing' (2018) <www.fin.gc.ca/activty/G7/pdf/G7-penetration-testing-tests-penetration-eng.pdf>.

resilience testing framework at this stage'[238] and that a multi-stage approach would be more appropriate in the EU context, starting with building a certain cyber resilience baseline.[239]

3. Licensing and certification

As part of the ongoing push for more comprehensive cybersecurity regulation, a number of regulators have designated certain types of cybersecurity activities as licensable. For example, in Singapore mandatory licensing applies to (i) managed security operations centre monitoring services and (ii) penetration testing services.[240] Although these activities are relevant for financial institutions, they are, at their core, sector-agnostic. In Russia, which also has a cybersecurity licensing framework,[241] the recent regulatory reform has made the use of licensed institutions mandatory for credit institutions and certain non-credit financial institutions, albeit to a different extent. The former are required to engage licensed entities for analysis of *vulnerabilities* in application software of automatic computer systems, starting from January 2020.[242] The latter must, from January 2021, engage third party licensed firms to verify *compliance* with the cybersecurity requirements applicable to them.[243] In addition, starting from January 2020, certain financial institutions (namely, money transfer operators and payment infrastructure operators) must ensure that application software used by them is certified by the Federal Service for Technical and Export Control (which includes, among other things, testing for undocumented features).[244]

---

[238] Joint Committee of the European Supervisory Authorities (n 220) 4.

[239] ibid 5. See also section VI(A) above.

[240] Singapore Cybersecurity Act 2018, Second Schedule.

[241] See Russian Government Regulation 79 of 3 February 2012 'On Licensing of Activities concerning Technical Protection of Confidential Data'.

[242] CBR Regulation 683-P, s 4.2 (effective from 01 January 2020).

[243] CBR Regulation 684-P, s 6.1 (effective from 01 January 2021).

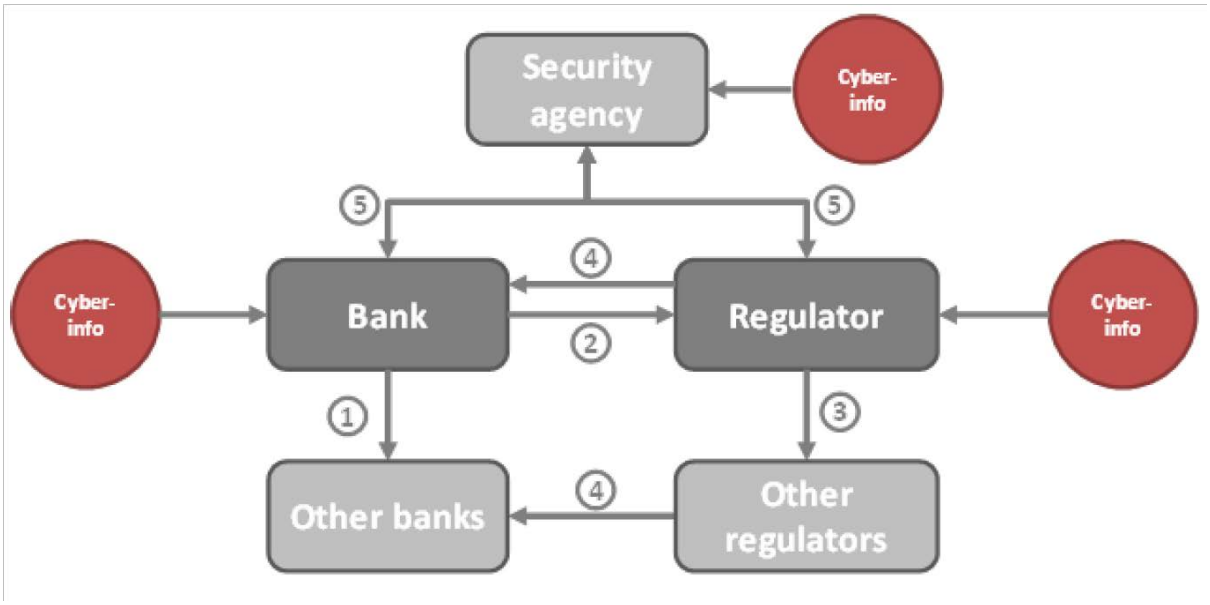
[244] CBR Regulation 382-P, s 2.5.5.1 (effective from 01 January 2020).

The EU has only taken the first steps towards a harmonised approach to European cybersecurity certification schemes in the form of a common framework, an initiative launched in parallel to enhancing the mandate of ENISA.[245] On a wider, international basis, the harmonisation of licensing cybersecurity regimes is likely to be infeasible in the absence of a common regulatory or certification scheme – given the diversity of existing standards in the area (see section V(B) above).

4. Cyber intelligence sharing

In addition to baseline reporting to regulators discussed in section VI(A), cybersecurity regulations may provide for a more comprehensive information-sharing regime involving a broad range of stakeholders, including, among others, financial regulators, dedicated cyber security regulators, security agencies and peer financial institutions. See Image 2.

Image 2. Interlinkage in different cybersecurity information sharing practices[246]



[245] Cybersecurity Act (n 31), Title III.

[246] Basel Committee (n 84) 22 (Figure 1).

Although a uniform regime for cyber intelligence information sharing may greatly enhance efficiency, international harmonisation in this area is fraught with challenges, such as confidentiality and the commercial sensitivity (sometimes even raising national security concerns) of cyber intelligence (eg in relation to existing cyber defences or vulnerabilities), lack of trust among various stakeholders (in particular among peers) as well as potential overlaps with existing restrictions (eg data protection rules).

Indeed, as noted elsewhere, cyber intelligence sharing is only in its early stages and it is safe to assume that any harmonisation should start with small steps, such as ensuring that different stakeholders are speaking the same language or making progress in areas where confidentiality is less of an issue.[247] However, the underlying problems noted above will not disappear, and regulators will have to address them one way or another, paying special attention to setting appropriate incentives for businesses (including non-compliance regimes). Some of the measures to help alleviate the issues may include (i) sharing anonymised data, (ii) disclosing relevant data only after the cyber incident has been resolved, (iii) separating internal (domestic) and international disclosure, to give the benefit of early disclosure to domestic stakeholders. Naturally, such measures sacrifice agility, but as is common in international harmonisation, sacrifices may be necessary to achieve an acceptable compromise. This said, delays in sharing of cyber intelligence are likely to forfeit much of its value: in an ideal world, such information would arrive quickly enough to flag potential imminent threats. However, fear of regulatory scrutiny or breach of existing obligations (eg under the GDPR) makes agile cyber intelligence sharing with regulators a challenge, highlighting the apparent conflict between data privacy and systemic stability that regulators will have to address. One possible response comes in the form of facilitating cyber

[247] D Domanski, 'Cyber Security: Finding Responses to Global Threats' (speech, 10 May 2019) <https://www.fsb.org/wp-content/uploads/S100519.pdf>.

intelligence sharing among firms without regulatory intervention – a model envisaged at the meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures in June 2019 in the form of the 'Cyber Information and Intelligence Sharing Initiative' (or 'CIISI-EU').[248]

5. Third party service providers

Interconnectedness of the financial sector means that, from a cybersecurity perspective, a small-value participant providing non-critical services could, in some cases, be as dangerous for the entire financial system as the largest payment service operator.[249] After all, smaller firms, which often do not have the resources to analyse the programming code for vulnerabilities, or negotiate appropriate contractual terms with software vendors or developers, are more prone to implementing 'black box' software that contains vulnerabilities and undocumented features. This means that risks associated with third party service providers cannot be ignored – especially in an international setting, whereby many third party services are provided on a cross-border basis. International harmonisation (at the sectoral as well as cross-sectoral level) is strongly desirable in this context.

Nonetheless, at the time of writing, cybersecurity requirements relating to third party service providers are largely non-existent – and where they are present, they remain extremely varied, despite the emerging international guidance.[250] One of the rare examples of explicit third party-related cybersecurity provisions is found in the NYCRR 500, and requires each regulated entity to have in place written policies and procedures to ensure security of

[248] See European Central Bank, 'Second meeting of Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)' (28 June 2019) 2-3 <www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/2019/20190628/2019-06-28_ECRB_summary.pdf>.

[249] See section II.

[250] See, eg, G7, 'Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector' (n 151).

information systems and non-public information accessible, or held by, third party service providers[251] (defined broadly as persons who are not affiliates of the regulated entity and provide services to it and have access to non-public information by providing such services).[252] These requirements are procedural and focus on risk identification, due diligence and periodic assessment of third party service providers. Although certain substantive cyber-defences are mentioned (including multi-factor authentication and encryption), these are only to be considered 'to the extent applicable'.[253]

In contrast, Russian law targets certain cybersecurity requirements of selected systemically important third party service providers. For example, in the context of the national Single Biometric System (SBS) used by individuals to access banking services that was launched in July 2018, regulators have established specific cybersecurity requirements not only for the banks transmitting biometric data into the system, but also for the system's operator (a telecoms operator 'Rostelecom'). For example, the SBS must ensure a standard of protection equal to 10^4 brute force access attempts per biometric sample.[254]

In the EU, in the light of the absence of relevant third-party requirements, the European Supervisory Authorities came up with a proposal 'to consider a legislative solution for an appropriate oversight framework for monitoring the activities of third party providers when they are *critical service providers* to relevant entities'.[255] It remains to be seen how the parameters of 'criticality' will be established (if this proposal is accepted) but cloud service

[251] NYCRR 500, s 500.11.

[252] ibid, s 500.01(n).

[253] ibid, s 500.11(b).

[254] Annex 3 to the Order 321 of 25 June 2018 of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation, s 4.

[255] Joint Committee of the European Supervisory Authorities, 'Joint Advice of the European Supervisory Authorities' JC 2019 26 (10 April 2019) 18 <https://eba.europa.eu/documents/10180/2551996/JC+2019+26+%28Joint+ESAs+Advice+on+ICT+legislative+improvements%29.pdf>.

providers are likely to be at the top of the list of third party service providers targeted by the prospective regulations. The latter are largely global players (such as Amazon, Microsoft and Google)[256] – suggesting that some form of global supervision may be useful but at the same time very difficult to establish (not to mention the fact that these providers are servicing multiple sectors).

VII. CONCLUDING REMARKS

Despite the wide range of international practices in regulating cybersecurity in the financial sector, it is clear from the analysis above that cybersecurity regulations still have a long way to go. A number of regulators are gradually moving away from abstract calls for greater security, and towards more sophisticated legal regimes. Still, such regulations remain scarce and are in their early stages.

Despite the progress achieved in a number of jurisdictions listed in this article, the way forward is fraught with many challenges:

1. Cybersecurity risks and responses should be better articulated – and treated separately from general operational risk concerns. Cybersecurity provisions should be less abstract and enhance legal certainty, particularly regarding the standard of diligence, liability and enforcement.

2. International harmonisation should be promoted by establishing a baseline set of requirements (including a common minimum standard for cyber event reporting). Lawmakers and regulators should be realistic when setting the baseline level and avoid

[256] L Dignan, 'Top cloud providers 2019: AWS, Microsoft Azure, Google Cloud; IBM makes hybrid move; Salesforce dominates SaaS' (ZDNet, 15 August 2019) <www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-salesforce-dominates-saas/>.

attempting early harmonisation of the more challenging aspects, such as wide-scale cyber intelligence sharing.

3. Without a clear cross-sectoral cybersecurity strategy, effectiveness of a cybersecurity framework in the financial sector is likely to remain limited, since some of the challenges can only be adequately addressed at an economy-wide, or even international, level.

4. The design of cybersecurity instruments does not have to be exclusively principles-based: regulators should aim to identify – and update on a regular basis – substantive requirements for cyber-defences (in dialogue with the industry, cyber experts and academia). When designing the regulatory landscape, it is helpful to analyse the relevant risks from the perspective of wilful misbehaviour of human actors and consider the limited usefulness of organisational measures in that context.

5. Competent authorities should not analyse the cyber risks of the financial system alone and need to consider the opportunities of cross-sectoral harmonisation (particularly in the context of TechFins and risks of third party service providers).

6. Risks of third-party service providers cannot be ignored, as they can be the source of contagion and proliferation of cyber risks within the financial system and beyond. The immediate threats include sources of data concentration, in particular cloud service providers and biometric databases. These service providers largely operate on a cross-sectoral (and often international) level, making it difficult to designate the regulator best placed to perform effective supervision.

7. The rapid pace of technological developments in cyberspace requires periodic review and updating of the current level of cybersecurity knowledge. Publication of thematic reviews on cybersecurity and other relevant materials, as well as promotion of pro-cybersecurity

culture at all levels, may assist not only in increasing the overall level of preparedness within the industry, but also in giving specific meaning to regulatory requirements containing references to 'state of the art' technologies and 'best practices' and ensuring that these innovations can be adequately implemented by competent personnel.

8. As the role of regulators in cyberspace increases, they should be mindful of the question, '*Quis custodiet ipsos custodes?*' ('*Who will watch the watchers?*') – and the need to consider their own cybersecurity risks. This is particularly relevant in the context of switching to systems-based reporting (and so-called big data) and the risks associated with insufficient in-house expertise.

9. Without adequate penalties and enforcement, cyber rules are likely to turn into unenforceable declarations. However, the special characteristics of cybersecurity threats make cyber enforcement extremely challenging, since the target's ability to thwart an attack is not always determined by the target's own actions (or inaction). In the absence of a coordinated regulatory response (which has already been called for within the information technology industry),[257] sanctioning individual firms is unlikely to remain effective or even justified in case of nation-state level cyber-attacks. In addition, regulators should also consider other (non-penalising) incentives to encourage compliance.

10. Finally, in designing cybersecurity rules, competent authorities should consider emerging international practices – an aspect in which this article will hopefully be of some use.

[257] See, eg, B Smith, 'The Need for a Digital Geneva Convention' (speech, 14 February 2017) <https://blogs.microsoft.com/wp-content/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf>.