FSB FINANCIAL STABILITY BOARD

Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices

13 October 2017

The Financial Stability Board (FSB) is established to coordinate at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations under the FSB's Articles of Association.

Contacting the Financial Stability Board
Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Table of Contents

1. Introduction

This is a summary report on financial sector cybersecurity regulations, guidance and supervisory practices ("Summary Report").

Cyber attacks are a threat to the entire financial system, a fact that is underscored by recent reports of significant and successful attacks both inside and outside the financial sector. The 2016 attack on the Bangladesh Bank resulted in the theft of $81 million, the WannaCry ransomware attack infected more than 250,000 computer systems in 150 countries, and the recent Equifax hack is estimated to have resulted in the compromise of personal information of up to 143 million individuals.[1] The changing nature of cyber risk to financial institutions is driven by several factors, including evolving technology, which can lead to new or increased vulnerabilities; interconnections among financial institutions and between financial institutions and external parties, e.g. through cloud computing and FinTech providers who may be outside the regulatory perimeter; determined efforts by cyber criminals to find new methods to attack and compromise IT systems; and the attractiveness of financial institutions as targets for cyber criminals seeking illicit financial gain.[2] Recognising the threat from cyber risks and the critical nature of enhancing financial institution resilience to those risks, authorities across the globe have taken regulatory and supervisory steps designed to facilitate both the mitigation of cyber risk by financial institutions, and their effective response to, and recovery from, cyber attacks.

The Communiqué issued at the March meeting of the G20 Ministers and Governors in Baden-Baden noted that the malicious use of Information and Communication Technologies could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability.[3] The Ministers and Governors further noted that they would promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of Information and Communication Technologies, including from countries outside the G20. With the aim of enhancing cross-border cooperation, the Ministers and Governors asked the FSB, as a first step, to perform a stocktake of existing relevant released regulations and supervisory practices in G20 jurisdictions, as well as of existing international guidance, including to identify effective practices. The FSB was asked to deliver a stocktake report ("Stocktake Report") by October 2017. The FSB initiated the requested stocktake in early April of this year by distributing two surveys to its members for

---

1 See https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8; http://www.bbc.com/news/technology-39913630; https://www.ft.com/content/2394ee58-9997-11e7-b83c-9588e51488a0.

2 For a discussion of cyber risk in the context of FinTech (e.g. technology-enabled innovation in financial services), see *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention*, http://www.fsb.org/2017/06/financial-stability-implications-from-fintech/.

For an example of the evolution of attack methods see https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/ for detail on the release of the source code for the Mirai botnet and http://www.gartner.com/newsroom/id/3436717 for detail on the predicted increase in Internet of Things devices.

For an outline of the high yield of recent attacks targeting the financial sector, see the section 'Targeted financial heists', https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf.

3 See http://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/g20-communique.pdf?__blob=publicationFile&v=3.

completion. One survey was directed to FSB member jurisdictions, and the second survey was directed to international bodies. The G20 request to the FSB was explicitly limited to **released** regulations, guidance and supervisory practices, and, as a result, the surveys were limited to publicly available materials. While regulations are typically published, supervisory practices may not be. Supervisory practices that are in use, but that have not been publicly released, were not covered by the G20 request or the FSB survey and are not reflected in the Stocktake Report. In addition, the survey was limited to regulations, guidance and supervisory practices issued by government authorities in each jurisdiction; it did not cover any guidance, supervisory practices or similar materials that may have been issued by self-regulatory organisations.

The jurisdiction survey requested information about existing publicly released regulations, guidance and supervisory practices that address cybersecurity for the financial sector, including financial market infrastructures (FMIs), trading venues, banks, insurance companies, broker-dealers, asset managers and pension funds.[4] The international body survey asked about guidance that has been issued that addresses cybersecurity for the financial sector, as well as other documents relating to cybersecurity, including studies, surveys and reports. All 25 FSB member jurisdictions responded to the survey.[5] The nine international body members that received the survey also responded.[6] In addition, the G7 Cyber Expert Group submitted a response to the survey.

In September of this year, the FSB held a workshop, which brought together public and private sector participants to discuss cybersecurity in the financial sector. Twenty-nine private sector participants were drawn from across the financial sector and related industries, including banks, insurance companies, broker-dealers, asset managers, exchanges, clearing organisations, technology firms and financial sector industry groups. The workshop provided senior officials from FSB members an opportunity to engage with chief information security officers (CISOs) and other senior leaders of firms concerning their views on effective practices in the area of cybersecurity and ways that authorities may contribute to enhancing cybersecurity throughout the financial sector. The workshop also provided a forum for members to discuss their experiences, across financial sectors and jurisdictions, in regulation and supervision with respect to cybersecurity.

The FSB's Stocktake Report and this Summary Report are informed by the responses of member jurisdictions and international bodies to the FSB's surveys. The Stocktake Report explores existing publicly released regulations, supervisory practices and guidance in the area of cybersecurity across the financial sector, including whether gaps exist and the degree of uniformity across the financial sector and FSB member jurisdictions. The Stocktake Report includes information concerning jurisdictions' self-reported existing publicly released

---

[4] For purposes of the FSB survey, generally "regulations and guidance" were defined as materials that impose requirements on, or provide guidance for, regulated entities; and "supervisory practices" were defined as practices that supervisory authorities or regulators use in their oversight or examination of regulated entities.

[5] The FSB member jurisdictions are Argentina, Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Korea, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Switzerland, Turkey, United Kingdom, United States and the European Union.

[6] This includes the Basel Committee on Banking Supervision, Committee on the Global Financial System, Committee on Payments and Market Infrastructures, International Association of Insurance Supervisors, International Accounting Standards Board, International Monetary Fund, International Organization of Securities Commissions, Organisation for Economic Co-Operation and Development and the World Bank.

regulations, guidance and supervisory practices; future plans; and views regarding effective regulatory and supervisory practices. The Stocktake Report also contains information regarding international bodies' self-reported guidance, other publications and future plans. This Summary Report includes summaries of the conclusions from the FSB's stocktake survey and key themes raised in the discussion at the September workshop.

2. Summary of FSB Survey Conclusions

The conclusions from the FSB's stocktake survey of members include the following.

FSB member jurisdictions have been active in addressing cybersecurity for the financial sector. All 25 member jurisdictions report that they have publicly released regulations or guidance that address cybersecurity for at least a part of the financial sector, and a majority have also publicly released supervisory practices. All or nearly all jurisdictions have addressed banks and FMIs, and a majority have addressed trading venues, insurance companies, broker-dealers and asset managers.

FSB member jurisdictions report a significantly higher number of publicly released regulatory schemes than publicly released supervisory practices schemes. It is important to note, however, that some supervisory practices may not have been publicly released, and therefore were out of scope of the stocktake.

International bodies also have been active in addressing cybersecurity for the financial sector. The 10 international bodies that responded to the FSB survey reported published guidance covering electronic banking; FMIs; firms and supervisory and regulatory authorities throughout the financial sector; critical information infrastructures, including financial sector actors that are critical information infrastructures; and all economic and social activities, across all sectors, from businesses, governments and individuals.

All FSB member jurisdictions report drawing upon a small body of previously developed national or international guidance or standards of public authorities or private bodies in developing their cybersecurity regulatory and supervisory schemes for the financial sector. This suggests that jurisdictions have found the existing guidance and standards to be useful and that there is some degree of international convergence in cybersecurity regulation and supervision of the financial sector.

The number of schemes of regulations and guidance addressing cybersecurity for the financial sector varied widely across jurisdictions. All member jurisdictions reported at least one regulatory scheme, with some reporting as many as 10. It is difficult to draw particular conclusions from the number of schemes reported. For example, there was no direct correlation between the number of schemes reported by a jurisdiction and the financial subsectors covered.

Jurisdictions reported that their regulatory schemes more commonly took a targeted approach to cybersecurity and/or IT risk (66% of reported schemes) and less commonly addressed operational risk generally (34% of reported schemes). By financial subsector, the percentage of reported regulatory schemes targeted to cybersecurity and/or IT risk ranged from a high of 83% for trading venues to a low of 60% for asset managers. For FMIs and banks, the percentages of reported targeted regulatory schemes were 77% and 71%, respectively.

Regulatory schemes categorised by jurisdictions as addressing operational risk often were characterised as principles-based, risk-based or proportional and specified the objectives to be met by regulated institutions. Nonetheless, many operational risk schemes enumerated a number of elements to be addressed by regulated institutions, commonly including governance; risk assessment and risk management; policies, procedures and controls; prevention, detection and reduction of vulnerability; protection of information; security tests; backup sites and disaster recovery; business continuity planning; notice to regulators; independent review; and third-party risks.

There were 56 schemes of regulations and guidance reported as targeted to cybersecurity and/or IT risk, which covered a variety of content elements. Some of the elements covered by those schemes, listed in descending order by the number of schemes in which they were included, are risk assessment (55); regulatory reporting (50); role of the board (49); third-party interconnections (49); system access controls (48); incident recovery (46); testing (44); training (43); creation of role responsible for cybersecurity, such as chief information security officer (38); information sharing (31); expertise of the board or senior management (22); and cyber risk insurance (15).

There were 35 schemes of reported supervisory practices, which covered a variety of content elements. Some of the elements covered by those schemes, listed in descending order by the number of schemes in which they were included, are review of policies and procedures (32); review of programmes for monitoring, testing and auditing (31); review of data security controls (31); review of governance arrangements (30); review of risk assessment process (30); review of past incidents and organisation's response and recovery (27); testing by supervisor and/or submission of test results to supervisor (21); communications by supervisor (21); review of sectoral impact of past incidents (21); information sharing by financial institutions (18); expertise of supervisory team (17); supervisory review of third parties (16); and joint public-private testing (14).

There are a number of similarities across international guidance, with many of the same topics addressed, even though there are considerable differences in the scope of entities covered and date of issuance of the guidance. Common topics addressed include governance; risk analysis and assessment; information security; security controls and incident prevention; expertise and training; monitoring, testing and/or auditing; incident response and recovery; communications and information sharing; oversight of interconnections; and continuous learning.

Jurisdictions remain active in the area of cybersecurity. Seventy-two percent of jurisdictions reported publicly released plans to issue new regulations, guidance or supervisory practices that address cybersecurity for the financial sector within the next year. These plans include engaging FMIs in a self-assessment exercise, developing a cybersecurity strategy and guidance for the financial sector and issuing new cybersecurity regulation.

Jurisdictions provided a wide range of responses when asked to cite practices that they deem effective in addressing cybersecurity through regulations, guidance and/or supervisory practices. Some items commonly cited were: specific, existing international guidance and standards; principles-based, risk-based or proportional supervision; the important role of the board and senior management; and communications, coordination and information sharing. Other items cited include independence of risk management, policies and procedures

concerning information systems management, identification and updating of cybersecurity requirements, strong control of outsourcing risks, assessment of cross-border and cross-sector threats and systemic risk, and a number of specific supervisory tools.

3. FSB Workshop on Cybersecurity

The summary below reflects some of the key themes raised in the discussion at the September workshop. It does not necessarily represent the views of authorities nor consensus views expressed by private sector participants at the workshop.

3.1 Effective Cybersecurity Practices

Private sector participants noted the **importance of establishing a firm's cybersecurity objective**, i.e. what the firm is trying to protect, because not all businesses are the same. For example, a firm that is in the business of providing access to publicly available data would be appropriately focused on the availability of that data rather than its confidentiality, whereas a firm with significant customer data would be appropriately focused on the confidentiality of that data. At the same time, however, private sector participants acknowledged that the goals of data integrity, availability and confidentiality do intersect.

Private sector participants noted that **effective cybersecurity requires a strategic, forward-looking, fluid and proactive approach**. They noted that it is not sufficient to simply look to past incidents and known risks, but that one must evaluate potential future threats. At the same time, participants stated that up to 90% of threats can be mitigated by basic cybersecurity hygiene.

Private sector participants noted the **importance of integrating security with business operations, as well as the importance of governance and communication with a firm's board**.

Private sector participants noted that **different types of testing and continuous monitoring all contribute to better cybersecurity**. This includes both self and third party testing. It also includes penetration testing, continuous monitoring, assurance and public-private sector tabletop exercises.

Private sector participants noted that cybersecurity is not simply about preventing cyber attacks. They stated that firms need to expect that controls and patches will fail at some point and that **institutions need to be resilient, i.e. they need to be ready to respond and recover from cyber incidents**. In this effort, people, processes and technology are all important, particularly that all three ought to be prepared to deal with changing circumstances.

Private sector participants discussed the impact of outsourcing on effective cybersecurity, noting that outsourcing could either increase or decrease risk, depending on factors such as internal capability to perform the outsourced function and how effectively outsourcing is managed. They noted the **importance of good outsourcing management, both at the contracting stage and on an ongoing basis**, by addressing issues such as appropriately limiting contractor access to confidential information, tailoring risk management based on consideration of the nature of the relationship with the vendor and where potential vulnerabilities lie, identifying backup suppliers in case a supplier fails, assessing security

management when selecting a contractor, being aware of and adequately managing the full length of the outsourcing chain, and incident reporting and resolution throughout the term of a contract. Participants also acknowledged potential risks arising from the highly concentrated market structure of providers of some services.

3.2 Effective Regulation and Supervision

Private sector participants acknowledged the importance of responding to the legitimate and growing needs of financial regulators and supervisors globally in the area of cybersecurity.

They expressed support for principles-based, risk-based and proportional regulation, as well as the cooperation between firms and regulators that is necessary in implementing principles-based regulation.

They advocated against prescriptive regulation and a compliance-focused approach, especially for large firms with sophisticated cybersecurity teams, expressing concern that it may provide a roadmap to criminals and that it may stifle development of more effective cybersecurity practices by industry participants. Some private sector participants, however, noted support for basic, prescriptive regulation of cybersecurity hygiene, which could form the main element of regulation for small firms and would be a foundational element of cybersecurity practices for large firms as well.

Private sector participants identified the following specific concerns about regulation and supervision of the financial sector and noted that there is currently no global process for coordinating regulation of cybersecurity.

Conflicting requirements. Private sector participants stressed the importance of regulatory harmonisation and a globally consistent approach, noting that multiple, potentially conflicting regulatory schemes impose costs and divert resources from operational cybersecurity at financial institutions. Participants noted that different regulatory requirements can drive structural changes in firms that are not optimal from a business standpoint, e.g. separating networks in different jurisdictions in order to insulate the parent and other subsidiaries from requirements that may be applicable to a single subsidiary. Specific areas where private sector participants identified different, and potentially conflicting, requirements include: timetables for required notification to regulators with respect to security incidents, penetration testing requirements, governance, data leakage protection and two-factor authentication requirements, as well as potential conflicts between privacy law requirements and cybersecurity requirements.

Similar, but not identical, requirements. Private sector participants stated that tracking of, and compliance with, multiple regulatory requirements is complicated even where those requirements are similar and do not conflict. An example cited was the use of seven sets of language under different regulatory schemes, in all cases implementing a single NIST control. Private sector participants also noted that regulators may use similar terms in their rules that may be interpreted differently across jurisdictions. In addition, deadlines for reporting cyber incidents differ from one country to another.

Unhelpful regulatory requirements. Participants expressed concern about regulatory requirements that, though well-intentioned, may not enhance cybersecurity. Examples cited were encryption requirements that may make it unduly difficult to search for cyber threats and a requirement that firms establish a "risk appetite" that lacks clarity on what is meant by "risk

appetite" in a cybersecurity context. A specific concern was raised that in some circumstances penetration testing from outside a firm could result in increased risk, either because testing could disrupt a network in a harmful manner or because hackers could gain access to test results. In addition, multiple penetration testing exercises may take resources away from other needed operations, such as monitoring for actual cyber attacks.

Authorities' Ability to Protect Firm Information. Private sector participants noted a concern about authorities' ability to protect financial institution information, indicating, for example, that some firms may be reluctant to provide regulators with specifics of some tools the firms use to address cybersecurity because they do not want this information in authorities' databases.

Examinations. Private sector participants expressed concerns about multiple similar, but slightly different, examinations by supervisors as imposing high costs. They also cited the need for better training of examiners.

3.3 Information Sharing

Both FSB member representatives and private sector participants in the workshop were of the view that information sharing is important in the area of cybersecurity. Participants generally expressed interest in enhanced cybersecurity information sharing although they did not discuss in detail who should share information, e.g. private firms among themselves, regulators among themselves and/or regulators and industry, or what information should be shared, e.g. threat intelligence, effective cybersecurity industry or regulatory practices and/or information about specific incidents. Private sector participants did note that information exchange between the private and public sectors is an important aspect of the public-private partnership, with some noting that information sharing should be permissive and protected, but not mandated. Both private and FSB member participants noted that cybersecurity is an inherently cross-border issue and that attacks can affect firms without regard to location. At the same time, both private and public sector participants acknowledged that setting up a cross-border architecture for information sharing presents a significant challenge, but a number of participants spoke to the importance of addressing this challenge as part of enhancing overall cybersecurity of the financial system.

3.4 Capacity Building: Cybersecurity Expertise and Awareness

Private sector participants noted the proliferation of cyber weapons and decreased costs for criminals to access attack tools. Against that background, they noted the comparative scarcity of cybersecurity trained professionals to help financial institutions respond. They cited the need to create capacity in this area and develop a pipeline of talent. As noted above, private sector participants also noted the need for better training of supervisory examination staff, while acknowledging that it is difficult for governments to compete with the private sector in attracting and retaining trained cybersecurity professionals.

Private sector participants also emphasised the importance of training at all levels within firms. They noted that the majority of successful cyber attacks involve human error and stressed the importance of awareness training for all staff. They also discussed the importance of educating the board about cyber risks.