

Financial Stability Institute

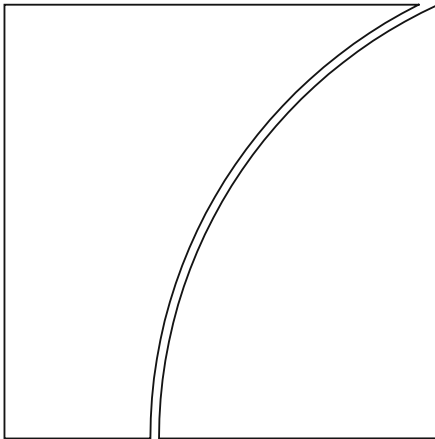
FSI Insights

on policy implementation

No 2

Regulatory approaches to enhance banks' cyber- security frameworks

By Juan Carlos Crisanto and Jermy Prenio



August 2017



BANK FOR INTERNATIONAL SETTLEMENTS

FSI Insights are written by members of the Financial Stability Institute of the Bank for International Settlements, often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of policy issues and implementation challenges faced by financial sector authorities. The views expressed in the FSI Insights are those of the authors and do not necessarily reflect the views of their respective institutions.

Authorised by the Chairman of FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please e-mail press@bis.org. You can sign up for e-mail alerts at www.bis.org/emailalerts.htm.

© Bank for International Settlements 2017. All rights reserved. Brief excerpts may be reproduced or translated provided the source is stated.

ISBN: 978-92-9259-080-2 (online)

Regulatory approaches to enhance banks' cyber-security frameworks*

Juan Carlos Crisanto (Bank for International Settlements)

Jermy Prenio (Bank for International Settlements)

* The authors are grateful to David Whyte, Head of BIS Cyber-security, for useful comments and suggestions, as well as to the financial sector authorities and industry participants who shared their perspectives on the issue.

Contents

Executive summary	1
Introduction	2
Developing specific regulations for cyber-risk.....	4
Existing key regulatory requirements relating to cyber-risk.....	5
Supervisory frameworks and tools	10
Observations about the implementation of cyber-risk regulations by the banking industry	12
Some policy considerations	15
References	17

Executive summary

Recent high-profile cyber-attacks on financial institutions have focused attention on the need to strengthen cyber-security. Among financial institutions, banks have the most public-facing products and services, and are thus significantly vulnerable to cyber-attacks. Consequently, cyber-risk is a major concern for most bank supervisors. However, only a handful of jurisdictions have specific regulatory and supervisory initiatives on banks' cyber-risk; these include Hong Kong SAR, Singapore, the United Kingdom and the United States. This paper therefore focuses on these jurisdictions in particular in its analysis of emerging regulatory and supervisory frameworks, with a view to drawing more general conclusions.

Views differ on the **need to specifically regulate cyber-risk**. One view is that the evolving nature of cyber-risk is not amenable to specific regulation and that cyber issues can be handled with existing regulation relating to technology and/or operational risk. The other view is that regulatory structure is needed to deal with the unique nature of cyber-risk, and given the growing threats resulting from an increasingly digitised financial sector.

For jurisdictions that already have specific **regulatory requirements**, a debate continues about the optimal level of prescriptiveness. Some jurisdictions favour a principles-based approach while others apply a more prescriptive framework. Despite these differences, the usual starting point for a cyber-security regulatory setup is to require banks to have a documented cyber-security programme or policy. Banks are expected to identify critical information assets that need to be protected. Testing banks' vulnerability and resilience to cyber-risk (such as through penetration testing) is a common requirement, as well as the reporting of cyber-events. Another common requirement relates to having clear responsibilities and accountabilities at banks as a key component of their cyber-security framework. Less common regulatory requirements include cyber-threat intelligence-sharing (although it is generally encouraged). The security capabilities of third-party providers are a critical element of any cyber-security framework but the specific supervisory approaches depend on the extent to which third parties are covered by the powers of bank supervisors.

Supervisory approaches specifically developed to assess the soundness of banks' cyber-security are still evolving. Cyber-security continues to be assessed largely as part of the ongoing risk-based supervisory framework and, more recently, this has been complemented by thematic reviews. However, supervisors seem to be converging towards undertaking a so-called "threat-informed" or "intelligence-led" testing framework, ie by using threat intelligence to design simulated cyber-attacks to test a bank's cyber-security. Also, it should be noted that an approach taken by some supervisors is to certify the information security professionals used by banks for their cyber-security activities. Attracting and retaining staff with cyber/information security expertise is a key challenge for supervisory authorities worldwide. There is also scope to increase the level of cooperation and coordination among supervisors from different jurisdictions and financial sectors.

Based on the range of practice it reviews, the paper offers some **high-level policy considerations**, which may be helpful for banking supervisory authorities contemplating or planning to introduce or enhance their cyber-security banking regulations or supervisory tools. These are, first, to incorporate cyber-risk, like any other bank risk, into the enterprise-wide risk management framework and governance requirements of supervised banking institutions. Second, to require banks to develop an effective control and response frameworks for cyber-risk, including ensuring the implementation of general sound risk management practices in the context of cyber-risk. Third, to consider as starting points the existing technical standards on cyber- and information security for any regulation relating to cyber-risk. Fourth, to put more emphasis in promoting cyber-security awareness among bank staff. Fifth, to benefit from further collaboration with the industry in strengthening banks' cyber-security. And, sixth,

to pursue greater cross-border cooperation and consistency in regulatory and supervisory approaches to enhance cyber-resilience at banks.

Introduction

- 1. Recent high-profile cyber-attacks on financial institutions have focused attention on the need to strengthen cyber-security, leading to various official sector initiatives to address cyber-risk.** At the international level, the G7 finance ministers and central bank governors issued a set of *Fundamental elements of cybersecurity for the financial sector*, with the aim of helping banks tailor their cyber-security approaches to their operational and regulatory environment.² The Financial Stability Board (FSB) included in its 2017 workplan³ the need to monitor cyber-risk arising from financial technology (fintech) and to identify the supervisory and regulatory issues from a financial stability perspective. The FSB's report for the July 2017 G20 Hamburg summit⁴ places the need to mitigate the adverse impact of cyber-risk on financial stability among the top three priority areas for future international cooperation. In June 2016, the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) issued *Guidance on cyber resilience for financial market infrastructures*.⁵ In April 2016, the International Association of Insurance Supervisors (IAIS) published an issues paper to raise awareness among insurers and supervisors of the challenges presented by cyber-risk.⁶
- 2. This increased attention to cyber-risk is not confined to the larger economies.** In 2016, the FSI conducted a survey of banking supervisors in 73 non-Basel Committee jurisdictions worldwide.⁷ In identifying their main macroeconomic and financial stability challenges, most respondents cited fintech and the resulting cyber-risk as their top challenge.
- 3. These concerns are shared by the industry.** The Deloitte's 2016 Global Risk Management Survey indicated that "only 42 percent of respondents⁸ considered their institution to be extremely or very effective in managing cyber-risk. Yet, cyber-risk is the risk type that respondents most often ranked among the top three that would increase in importance over the next two years (41 percent)".⁹ In January 2017, Risk.net ranked cyber-risk as the topmost among the top 10 operational risks for 2017. This ranking was based on interviews with chief risk officers, heads of operational risk and

² See US Treasury (2016).

³ See Financial Stability Board (2016).

⁴ See Financial Stability Board (2017).

⁵ See CPMI-IOSCO Guidance (June 2016).

⁶ See International Association of Insurance Supervisors (2016).

⁷ See Raskopf et al (2016).

⁸ Seventy-seven financial institutions from around the world and across multiple financial services sectors, representing a total of US\$ 13.6 trillion in aggregate assets.

⁹ See Deloitte (2016).

other operational risk practitioners at financial institutions, including banks, insurance firms and asset managers.¹⁰

4. **The CPMI-IOSCO Guidance defines “cyber-risk” as “the combination of the probability of an event occurring within the realm of an organisation’s information assets, computer and communication resources and the consequences of that event for an organisation”.**¹¹ By this definition, any organisation (or person) with information assets and uses online communications technology is exposed to cyber-risk. Indeed, the advent of information technology (IT) has made interconnections of people and organisations within and across economies pervasive, and with this comes the heightened risk of cyber-attacks.
5. **A number of jurisdictions are putting in place national policies or frameworks for strengthening the cyber-security of critical sectors and institutions.**¹² The financial sector is not only a critical sector but, arguably, it is more exposed to cyber-risk than other sectors, given that it is IT-intensive and highly dependent on information as a key input. Financial firms are also highly interconnected (including with other sectors) through the payment systems. The financial sector also provides products and services that are time-critical, which could be undermined by a cyber-attack.
6. **Within the financial sector, banks typically have the most public-facing products and services.** Bank systems’ multiple points of contact with outside parties result in significant vulnerability to cyber-attacks, and could be used as entry points for attacks targeting other parts of the financial system. Hence, it is important that banks have adequate governance, systems, procedures and processes in place to mitigate cyber-risk.
7. **While cyber-risk is a major concern for most bank supervisors, only a handful of jurisdictions have specific regulatory and supervisory initiatives to address banks’ cyber-risk.** This paper presents the emerging regulatory and supervisory approaches to address banks’ cyber-risk¹³ with a particular focus on the work of a few leading jurisdictions. First, the paper explores the different views on the regulation of cyber-risk, as well as existing key regulatory requirements and supervisory approaches implemented or proposed in leading jurisdictions. It then discusses cyber-security implementation issues from the banks’ perspective. Finally, the paper offers some policy considerations in implementing regulatory and supervisory approaches to enhance banks’ cyber-security frameworks.

¹⁰ See Risk.net (2017).

¹¹ See CPMI-IOSCO Guidance, June 2016.

¹² For example, Singapore’s Cyber-security Strategy, Canada’s Cyber Security Standard, the US Department of Homeland Security’s different initiatives to protect US critical infrastructure, South Africa’s National Cyber-security Policy Framework (NCPF); the Critical Infrastructure Protection in France.

¹³ IT or operational risk-related regulations or guidelines in some jurisdictions seek to capture cyber-risk along with other risk types under IT and operational risks. This paper focuses only on banking regulations or guidelines specifically targeting cyber-risk.

Developing specific regulations for cyber-risk

8. **There are two extreme views on the regulation of banks' cyber-risk: one which sees no need for specific regulations, and the other which favours specific regulations.** In the former, cyber-risk is viewed as any other risk and thus the general requirements for other risks (eg governance, setting of risk appetite etc) also apply. This view perceives the evolving nature of cyber-risk as not amenable to specific regulations, which would only become outdated and ineffective.¹⁴ Regulations may also result in a compliance-based approach to dealing with cyber-risk. The latter view, on the other hand, emphasises the importance of providing structure through the regulation of cyber-risk in order to properly cope with its specificities and its growing relevance given the increasingly digitised nature of finance. In fact, specific regulations on cyber-risk are fairly recent and have been either introduced or proposed only in the last few years. In general, these are meant to supplement the more general regulations on IT.
9. **One potential benefit of regulation is that it can help ensure board and management buy-in.** As regulation makes any issue more visible to boards and management, regulation on cyber-risk gives banks a stronger incentive to continuously invest in improved cyber-security. Banks' boards and senior management have the natural incentive to ensure sound cyber-security given the potentially damaging monetary and reputational costs of cyber-attacks. However, boards and senior management may not always be forward-looking and may not appreciate the business implications of cyber-risk, and hence be inclined to subordinate cyber-resilience to other business objectives in the absence of regulation.
10. **However, the risk exists that regulation becomes too prescriptive, so that it falls behind both the constantly evolving threat from cyber-risk and advances in cyber-risk management.** While prescriptive rules may be necessary in some areas, for example, by requiring banks' boards to establish a cyber-risk management framework and appetite, other areas are clearly less suitable for specific rules. Prescribing the use of a specific technology is one example; given the rate of technological change, any prescribed technology is likely to become rapidly outdated. Mandating a specific recovery time is another example where regulators need to be careful how banks go about implementing it. The aim is to prevent the lengthy disruption of critical financial operations, but an excessively stringent and rigid recovery time may prove counterproductive if this comes at the expense of banks' ability to thoroughly check that all their systems are no longer compromised.
11. **Existing technical standards on cyber and information security could be a valuable starting point for any regulatory guideline.** For instance, in 2013–14, the US National Institute of Standards and Technology (NIST) developed a cyber-security framework in close cooperation with the private and public sectors. Consisting of a set of industry standards and best practices that help organisations manage cyber-risk, the framework is used voluntarily by organisations across the United States and has also received significant worldwide attention. As such, the NIST framework could be a valuable starting point for jurisdictions that decide to put in place or upgrade their approach to cyber-security. Other influential technical standards in the cyber/information security community include the Center for Internet Security (CIS) Controls¹⁵ (which maps into the NIST

¹⁴ See eg Gracie (2014).

¹⁵ See CIS Security.

Framework), and the International Electrotechnical Commission (ISO/IEC) 27000 series.¹⁶ Otherwise, adoption of regulatory guidelines that differ considerably with existing technical standards could lead to confusing or conflicting approaches and result in unnecessary duplication of effort, leaving less resources for actual protection activities.

12. **The cross-border nature of cyber-threats requires a high degree of alignment in national regulatory expectations.** Given the borderless nature of cyber-crime, no single firm or regulator can successfully tackle the risk alone. The international nature of cyber-risk will not only require a collaborative response from governments, regulators and industry but also a high-degree of alignment across national regulatory frameworks. The *G7's Fundamental elements* is a step in the right direction. However, there is still much work to do in this area. Differing regulatory frameworks for cyber-risk across jurisdictions have the same impact as regulations that are in conflict with existing technical standards. For banks operating in various jurisdictions, alignment of regulatory expectations would help them avoid conflicting guidance, some of which would be undertaken simply for compliance purposes without any real improvement in cyber-security.

Existing key regulatory requirements relating to cyber-risk

13. **This section and the next are based mainly on the regulation and supervision of banks' cyber-risk in Hong Kong SAR, Singapore, the United Kingdom and the United States.**¹⁷ These jurisdictions were chosen for (i) their specific regulatory and supervisory initiatives on banks' cyber-risk and (ii) their leading role in coming up with a comprehensive approach to promoting cyber-resilience. The cyber-risk frameworks in these jurisdictions have been analysed using publicly available information, supplemented by interviews with relevant authorities, and by comparing these cyber frameworks with the approaches taken by other jurisdictions.¹⁸
14. **For jurisdictions with specific regulatory requirements for cyber-risk, the usual starting point, as with any other general regulation on other risks, is for banks to have a documented cyber-security programme or policy.** The requirements typically follow the CPMI framework's risk management categories involving governance, identification, protection, detection, response and recovery (see Box 1). Hence, these include general requirements on governance and oversight, risk ownership and accountability, information security measures (eg patch management procedures, access controls, identity management etc), periodic evaluation and monitoring of cyber-security controls, incident response, business continuity and recovery planning.
15. **Banks in the jurisdictions covered in this report are expected to be able to identify their critical information assets.** At the national level, governments identify critical infrastructure and firms to which their national cyber-security frameworks apply. Banks are expected to do the same

¹⁶ See International Organisation for Standardization and the International Electrotechnical Commission (2016).

¹⁷ For the United States, the paper looks at both the final regulation issued by the New York State's Department of Financial Services (DFSNY) and the proposed cyber regulation from the Federal regulatory agencies (ie the Federal Reserve Board, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation). However, interviews were conducted with officials of Federal agencies only.

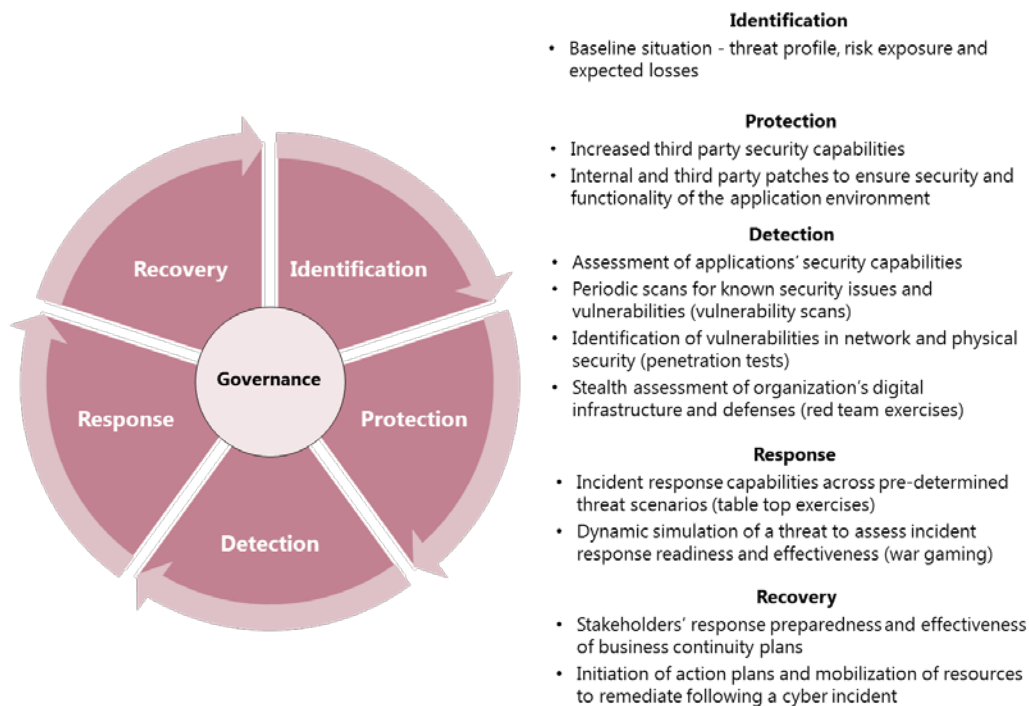
¹⁸ This included a review of publicly available information for Ireland and the Netherlands. In addition, we had discussions with regulators from one jurisdiction each in Africa and Latin America to seek views from other regions.

at their own level. This enables the prioritisation of cyber-security efforts on systems that contain critical information assets. Ideally, the entire bank should be protected but, given limited resources, banks should be able to target where to deploy their resources to maximise the benefits. Legal and regulatory requirements relating to data protection are the usual starting points for the identification of critical information assets.

16. **Testing banks' vulnerability and resilience to cyber-risk is a common requirement in the jurisdictions covered.** For instance, penetration testing involves not just identifying vulnerabilities of banks' systems but also "the use of a variety of manual and automated techniques to simulate an attack on an organisation's information security arrangements".¹⁹ Some tests go further by using cyber-threat intelligence in designing these simulated attacks. For their part, banks are fully aware of the importance of such tests. In fact, the Association of Banks in Singapore (ABS) has taken the lead in establishing guidelines to be followed in the conduct of the regulatory required penetration testing. In at least one jurisdiction, banks are said to be conducting penetration testing on their own initiative, even though no regulatory requirement is yet in place. The issue of penetration testing as a tool for supervisory assessment of cyber vulnerability and resilience is covered in more detail in the next section on supervisory frameworks and tools.

¹⁹ See Council for Registered Ethical Security Testers (2017).

Emerging cyber-security framework



Sources: CPMI-IOSCO (2016); Oliver Wyman's approach as described in Mee and Morgan (2017).

17. **Cyber-event reporting is another common regulatory practice.** Some jurisdictions have specific requirements for the regulatory reporting of cyber-events, subject to materiality (eg if the impact is deemed to be material enough to adversely impact the bank's operations) or the event posing risk to a bank's critical systems. In other jurisdictions, cyber-events are already captured in existing reporting requirements (eg events mandated by law or existing regulation to be reported to a government body or regulatory agency).²⁰
18. **Cyber-threat intelligence-sharing may not always be an explicit regulatory requirement, but it is encouraged.**²¹ Only Hong Kong includes an explicit requirement in its Cybersecurity Fortification Initiative (CFI), by incorporating an element of effective infrastructure for sharing intelligence in which all banks are expected to participate (see Box 2). In one jurisdiction, while

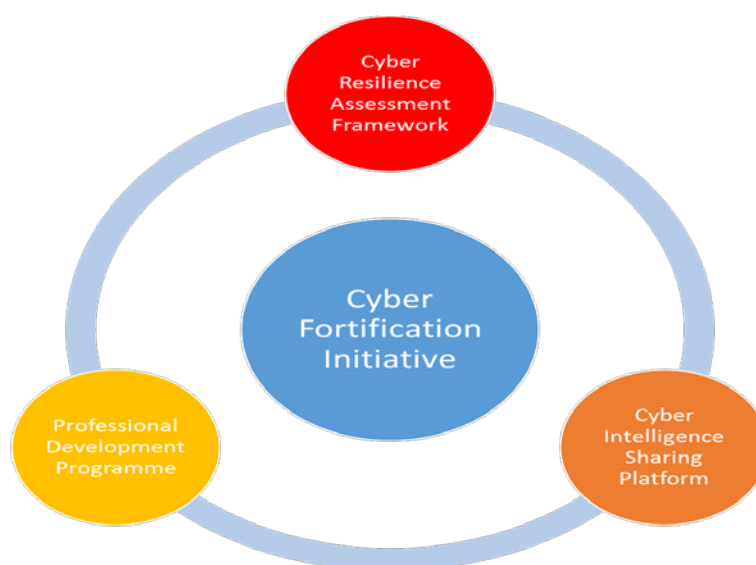
²⁰ For example, the US Treasury Department's Financial Crime Enforcement Network (FINCEN) issued an Advisory on 25 October 2016 advising financial institutions to include cyber-related events in their Suspicious Activity Reports (SARs).

²¹ It should be noted that the G7's *Fundamental elements of cybersecurity for the financial sector* includes information-sharing.

information-sharing is not explicitly included in its regulations, banks are “strongly encouraged” to participate in a sharing platform maintained by the regulator. In other jurisdictions, banks are encouraged to participate in security information-sharing forums. Financial firms have also taken the initiative to establish their own efforts in this regard.²² In addition, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) has established a Customer Security Programme (CSP) that requires, among other things, that user institutions share all relevant information as soon as possible if they have been targeted or breached. This forms part of their contractual obligations as SWIFT users.

Box 2

The Hong Kong Monetary Authority's (HKMA's) Cybersecurity Fortification Initiative



The HKMA's Cybersecurity Fortification Initiative (CFI) has three main elements:

- i. Cyber Resilience Assessment Framework – includes an inherent risk assessment, maturity assessment, and an intelligence-led cyber-attack simulation testing (ICAST);
- ii. Professional Development Programme – seeks to increase supply of qualified cyber-security professionals in Hong Kong; HKMA is working with the HK Institute of Bankers and the HK Applied Science and Technology Research Institute (ASTRI) to develop a localised certification scheme and training programme for cyber-security professionals; and
- iii. Cyber Intelligence Sharing Platform – seeks to provide an effective infrastructure for sharing intelligence on cyber-attacks; being set up by the HKMA together with the HK Association of Banks (HKAB) and ASTRI.

Source: HKMA: Cybersecurity Fortification Initiative, 24 May 2016; graphic by FSI.

²² For example, through the Financial Services Information Sharing and Analysis Center (FS-ISAC), www.fsisac.com.

19. **While regulators commonly expect clear accountability within banks for cyber-risk issues, a specific requirement to designate a Chief Information Security Officer or equivalent is less widespread.** Regulatory requirements with regard to banks' documented cyber-security programme or policy include a governance framework for cyber-risk, ie clear assignment of cyber-risk management responsibilities relating to identification, protection, detection, response and recovery. But regulatory requirements usually stop short of mandating banks to designate a Chief Information Security Officer (CISO). One possible reason is the lack of information security professionals who could fill this position. In fact, the requirement issued by the New York State's Department of Financial Services (DFSNY), for example, allows the CISO to be employed by a third-party service provider (ie not an employee) of the bank, subject to certain conditions.²³ In one jurisdiction, only "critical" banks are required to designate an information security officer.
20. **The security capabilities of third-party providers are a critical element of any cyber-security framework but jurisdictions have different regulatory approaches to deal with this issue.** Third parties are widely used by banks to provide services, systems or IT solutions that support banks' operations. Use of the public cloud, for example, is one recent innovation. As a consequence, non-public information may be held by or accessible to third parties. Cyber-related requirements relating to this issue are dependent on the extent to which third parties are covered by bank supervisory powers. Authorities in most jurisdictions put the onus on banks to ensure that the third parties they deal with have the same stringent security policies, procedures and controls that the regulators expect of regulated firms. The US authorities, however, have oversight of third-party firms and can therefore assess for themselves the soundness of cyber-security in these firms.²⁴ This is on top of specific requirements for US banks' interaction with third-party service providers. In other jurisdictions, they require service level agreements (SLAs) between banks and outsourcing companies to include a clause that allows supervisors to examine the latter's systems. With regard to the conduct of penetration testing, at least in one jurisdiction, third-party firms are only in scope if there is explicit consent.
21. **Some regulators certify the information security professionals used by banks for their cyber-security activities.** One reason is the sensitive nature of these activities, given that the people involved will gain insights into a bank's defences. The United Kingdom, for example, has established CBEST accreditation for any information security professionals involved in CBEST testing. This is in addition to the Council for Registered Ethical Security Testers (CREST) accreditation established by the industry. Another reason is the limited number of information security professionals in most jurisdictions. In Hong Kong, this is being addressed by including a Professional Development Programme (PDP) in its CFI. While the PDP is a local certification and training programme, its aim is to increase the supply of qualified cyber-security professionals. The scarcity of qualified people in this area is also reflected in the DFSNY regulation that allows banks to use cyber-security professionals employed by third parties. The problem, though, is not only about the limited availability of people with technical knowledge of cyber-security. A further problem is the limited cyber-security awareness of staff within banks, which itself could potentially open the way for a

²³ See DFSNY (2017).

²⁴ In the United States, the Bank Service Company Act (BSCA), 12 U.S.C. §1867(c) authorises the federal banking agencies to regulate and examine the performance of certain services by a third-party service provider for a depository institution "to the same extent as if such services were being performed by the depository institution itself on its own premises".

cyber-event. However, few jurisdictions explicitly require cyber-security awareness training for all bank staff.

Supervisory frameworks and tools

22. **Supervisors have traditionally assessed cyber-security as part of their ongoing risk-based supervisory activities, complementing these more recently with thematic reviews.** The traditional supervisory approach to assessing cyber- or IT risks in general is to include such assessments, whether by the supervisor or the bank itself, within the ongoing risk-based examination. This typically involves evaluating whether banks meet a series of criteria, assigning a rating and then, based on that rating, determining any management or regulatory actions. More recently, some authorities have used thematic reviews on cyber-security as a complement to their supervisory work. These reviews are generally based on information related to IT- or cyber-security incident reports and previous examination deficiencies. The purpose is to help regulators to identify and analyse trends across institutions so that they can better target areas for review at the subject institutions.²⁵ This type of complementary approach has enabled the ECB's Single Supervisory Mechanism (SSM) to include a dedicated section in its methodology for on-site inspections, develop new analytical tools for off-site supervisors, and produce a cyber-risk profile for each bank within its remit.²⁶
23. **Supervisors are converging towards a threat-informed or intelligence-led testing framework for assessing cyber-risk vulnerability and resilience.** An intelligence-led framework goes beyond a simulated cyber-attack to test a bank's cyber-risk vulnerability and resilience. Under this framework, the simulated attack is not just a random hacking attempt but one based on what cyber-threat intelligence sees as the probable target systems of the bank and attack methods (hence, "threat-informed" or "intelligence-led"). Banks are then assessed on the quality of the intelligence gathered, as well as their detection and response capabilities, to establish whether their level of cyber-security is commensurate to the cyber-risk faced. A remediation plan is then devised, as appropriate. The United Kingdom's CBEST framework is a good example of this approach (see Box 3). Other jurisdictions are implementing a similar approach, modified as needed to suit local specificities.²⁷ However, for most jurisdictions adoption of this approach could prove challenging, given the general scarcity of the two critical elements that must be present for this approach to be effective: (i) experienced cyber/information security professionals and (ii) sound cyber-threat intelligence.
24. **Supervisory frameworks or tools to assess cyber-risk vulnerability and resilience can be either voluntary or mandatory, for all or selected banks.** The US National Institute of Standards and Technology (NIST) Cyber-security Framework (CSF) and the Federal Financial Institutions Examination Council (FFIEC) Cyber-security Assessment Tool (CAT) are both voluntary tools that

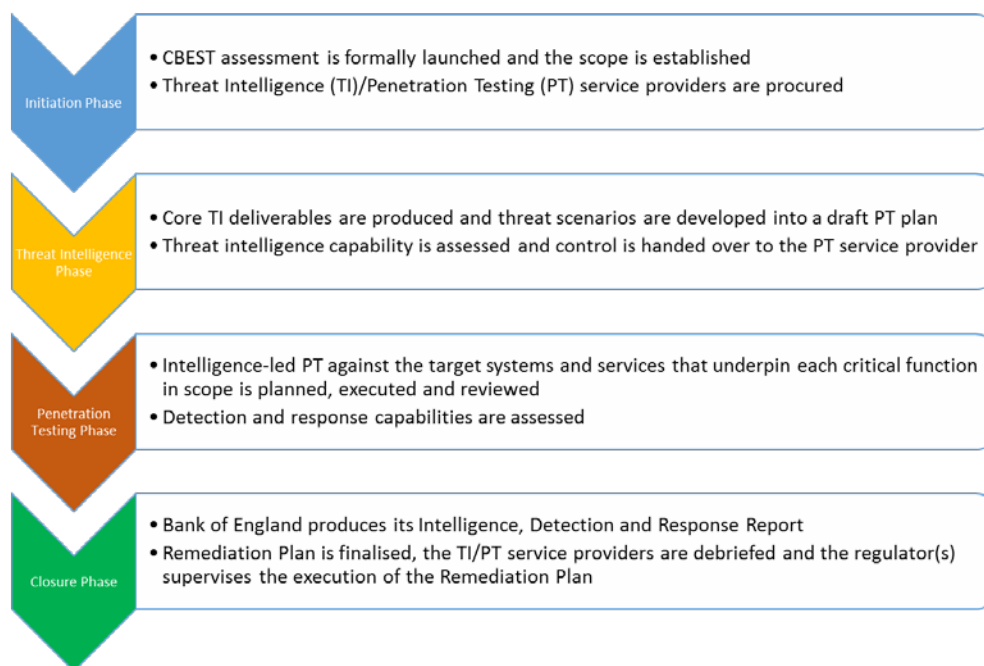
²⁵ See US Government Accountability Office (2015).

²⁶ See Lautenschläger (2017).

²⁷ For example, the Hong Kong Monetary Authority's iCAST (intelligence-led Cyber-attack Simulation Testing) Framework and the Netherland Bank's TIBER (Threat Intelligence-Based Ethical Red Teaming) Framework.

banks can use to assess cyber-risk.²⁸ The United Kingdom’s CBEST framework is also a voluntary programme for firms and financial market infrastructures (FMIs) that are considered core to the UK financial system.²⁹ By contrast, Hong Kong’s Cyber Resilience Assessment Framework (C-RAF) is mandatory for all institutions authorised by the Hong Kong Monetary Authority. Moreover, penetration testing is also a requirement for all banks in Singapore, where as mentioned the ABS has taken the lead in establishing the guidelines to support the implementation of the regulatory requirement.

The Bank of England’s CBEST framework



Source: Bank of England, CBEST Intelligence-Led Testing, CBEST Implementation Guide, Version 2.0; graphic by FSI.

25. **Attracting and retaining staff with cyber/information security expertise is a key challenge for supervisory authorities worldwide.** In 2015, the US Government Accountability Office reported³⁰ that, while the country’s largest deposit-taking institutions were generally examined by IT experts, medium and smaller institutions were sometimes reviewed by examiners with little or no IT training. According to the same report, US regulators recognised that, as some IT training is necessary for all examiners, efforts were under way to increase the number of staff with IT expertise and conduct more training. More generally, the 2017 Global Information Security Workforce Study,³¹ covering

²⁸ The NIST CSF is industry-neutral, while the FFIEC is based on the former but modified for use by financial firms.

²⁹ Although voluntary, all banks in the CBEST list, except one, have already undertaken the programme. The last bank is expected to do so by the end of the year.

³⁰ See US Government Accountability Office (2015).

³¹ See Booz Allen Hamilton, Center for Cyber Safety and Education, and ISC (2017).

2,620 cyber-security professionals in the US federal government, reported that almost 70% of respondents indicated not having the staff necessary to address cyber-threats, explaining that this was due mainly to difficulties in finding qualified personnel and retaining information security workers. The same study reports that the three most effective incentives for attracting and retaining cyber-security staff are (i) offering training programmes or paying for security certification; (ii) improving compensation packages; and (iii) flexible work schedules.

26. **Supervisory cooperation and collaboration is important in dealing with cyber-risk.** Supervisors in different jurisdictions appear to be actively exchanging practices, but there is scope for more supervisory cooperation and collaboration. For example, in cases where supervisors in different jurisdictions have an interest in the same critical business functions or systems of an internationally active bank, it is reasonable to expect supervisory cooperation and collaboration in testing the vulnerability and resilience of these functions or systems to cyber-attacks. This could take the form, for example, of undertaking joint penetration testing in order to avoid multiple tests that would be overly burdensome for banks and could divert cyber-security resources.

Observations about the implementation of cyber-risk regulations by the banking industry

27. **Leading banks are actively strengthening their cyber-security, recognising the reputational and monetary implications of cyber-attacks.** This section builds on discussions with industry practitioners on initiatives to strengthen cyber-security. It starts by focusing on governance-related challenges, then presents a perspective from banks on cyber-risk regulations and the role of the government.
28. **As with any important undertaking, buy-in at the top is necessary for banks' cyber-security initiatives to gain traction.** Banks' boards should appreciate the importance of cyber-security for their businesses (see Box 4). This is not so much about having people on the board who understand the technical details of cyber-risk, rather it is more about communicating cyber-risk information in a language that the board understands (ie financial rather than technical). This involves translating cyber-risk into money terms – ie what are the likely losses of a bank in the event of a cyber-attack?
29. **Since cyber-risk affects all parts of a bank's structure, management must take an enterprise view of cyber-risk and establish clear accountabilities.** A siloed approach to managing cyber-risk will obscure where accountability for cyber-risk falls (eg should fraud or financial crimes units within the bank be responsible?). The common practice is to assign a CISO or equivalent to oversee bank-wide cyber-security. In some cases, the CISO reports to the Chief Risk Officer (CRO), in others to the Chief Information Officer (CIO). The former case would seem to be the natural choice since all of a bank's risks should be within the CRO's remit. However, CROs usually do not have a technology background and thus may not view cyber-risk as part of their remit, which may be narrowly defined as including only the traditional financial risks. CIOs, on the other hand, are familiar with technology but their position in business operations creates a conflict with the review function of risk management (ie having the first and second lines of defence under one person or function). Nevertheless, anecdotal evidence suggests that leading financial institutions assign ultimate responsibility for cyber-risk and the CISO to the CRO.

Board principles for cyber-resilience

As part of the World Economic Forum's Initiative on the Digital Economy and Society, the Forum partnered with the Boston Consulting Group and Hewlett Packard Enterprise to identify a comprehensive framework that boards of directors can use to smoothly integrate cyber-risk and resilience into their firms' business strategy. This framework is summarised below.

Principle 1

Responsibility for cyber-resilience. The board as a whole takes ultimate responsibility for oversight of cyber-risk and resilience. The board may delegate primary oversight activity to an existing committee (eg the risk committee) or a new committee (eg a cyber-resilience committee).

Principle 2

Command of the subject. Board members receive cyber-resilience orientation on joining the board and are regularly updated on recent threats and trends.

Principle 3

Accountable officer. The board ensures that one corporate officer is accountable for reporting on the organisation's capability to manage cyber-resilience and progress in implementing cyber-resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

Principle 4

Integration of cyber resilience. The board ensures that management integrates cyber-resilience and cyber-risk assessment into the overall business strategy and enterprise-wide risk management, as well as budgeting and resource allocation.

Principle 5

Risk appetite. The board annually defines and quantifies business risk tolerance relative to cyber-resilience and ensures that this is consistent with corporate strategy and risk appetite.

Principle 6

Risk assessment and reporting. The board holds management accountable for reporting a quantified and comprehensible assessment of cyber-risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber-Risk Framework.

Principle 7

Resilience Plans. The board ensures that management supports the officer accountable for cyber-resilience by the creation, implementation, testing and ongoing improvement of cyber-resilience plans, which are appropriately harmonised across the business. It requires the officer in charge to monitor performance and regularly report to the board.

Principle 8

Community. The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber-resilience.

Principle 9

Review. The board ensures that a formal, independent cyber-resilience review of the organisation is carried out annually.

Principle 10

Effectiveness. The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement.

Source: World Economic Forum, *Advancing cyber resilience - principles and tools for boards*, January 2017.

30. **Leading banks recognise that it is a question of *when*, not *if*, they will experience a cyber-attack.** This "assume breach" mentality is now replacing the traditional concept of building a strong

perimeter to ward off a cyber-attack. The new threat environment, characterised by multiple points of potential entry for attacks, has reduced the effectiveness of the traditional security approach that relies solely on marshalling all of an institution's security devices/detective capability to guard the perimeter. The assumption of breach approach complements the traditional measures with intrusion detection techniques as well as response measures (eg to prevent the extraction of critical data).

31. **Raising cyber-security awareness among bank staff is an important component of a bank's initiative to protect itself from cyber-risk.** In essence, cyber-security is less about technology and more about people (eg it is people, not computers, who click on suspicious links). But there has been too much focus on technology solutions, and less so on people and processes. Leading financial institutions are investing to raise cyber-security awareness among all staff, in particular helping frontline personnel to understand the value of the assets they use every day. These institutions have put in place a set of mechanisms that encourage and enable staff to interact with the company's technology environment responsibly.³² Leading institutions are also seeking ways to measure staff cyber-security awareness (eg by sending "suspicious" links to bank staff and counting the number of clicks before and after a cyber-security awareness training). In undertaking these initiatives, using the right language is critical, just as it is when communicating cyber-risk to the board. One of the biggest obstacles to cyber-security awareness is that people do not know the language and thus are discouraged from asking questions and getting involved in the discussion. Hence, cyber-security awareness should be communicated to staff in language they understand, eg the potential cyber-risk they face on a daily basis.
32. **Although industry views seem split on whether specific regulatory and supervisory guidance on cyber-risk adds value, there is concern about the increasing number of duplicative and inconsistent regulations and guidance.** One view is that regulatory and supervisory guidance is not needed, since technical standards on cyber or information security already exist. The view here is that banks already own the risk of cyber-attacks and have every incentive to mitigate it. This argument rests on a rather strong assumption that, when faced with the cost implications of building a strong cyber-security, banks' boards and management would always prioritise cyber-security at the expense of competing business objectives. The second view, however, accepts that cyber-attacks are part of the operational risks that banks face on a daily basis and, hence, regulators and supervisors have an interest in ensuring that proper controls, policies and processes are in place. However, holders of both viewpoints agree that the technical details of cyber-security standards should be left with the technical standard setters and not with banking regulators. Related to this, a key concern voiced by industry practitioners relates to the number of duplicative and inconsistent regulations and guidance that substantially increase the banks' compliance burden and divert scarce resources from cyber-security activities to mere regulatory compliance exercises. In response, some industry initiatives are seeking to come up with a singular cyber-security framework and taxonomy that addresses supervisory requirements while preserving banks' ability to implement the most effective cyber-security approach for their own operating environment.³³

³² See Kaplan et al (2015).

³³ For example, the efforts by financial trade associations in the United States to come up with a financial services sector cyber-security profile. The idea behind this profile is to achieve a more harmonised regulatory approach for the financial services sector by using the approach and organisation of the NIST Cyber-security Framework, but customising it in a way that maps key regulatory requirements onto the five NIST categories of Identify, Protect, Detect, Respond and Recover.

33. **Cyber-security is viewed as within the remit of national governments, which should have an active role to play in the broader cyber-defence structure.** In the four jurisdictions covered, as well as in most other jurisdictions, a national framework is already in place to strengthen the cyber-security of critical sectors and infrastructure. Hence, governments are already playing an active role in the national cyber-defence structure. However, with the growing importance of a threat-informed and intelligence-led framework for assessing cyber-risk vulnerability and assessment, banks believe that consideration must be given to the role of governments in providing cyber-threat intelligence, given that it has become somewhat of a public good. This should, of course, take into account the legal as well as national security implications of such actions. The current practice is for banks themselves to source intelligence from open sources, with the government in some cases checking its quality. While information-sharing initiatives are already in place, which may be either mandated by regulators or industry-led, such pooled information may be of limited value for “intelligence-led” testing purposes since cyber-threats differ from institution to institution.

Some policy considerations

34. **Any cyber-security framework should be aligned with the overall operational risk and enterprise-wide risk management strategy.** A successful cyber-attack is very likely to affect people, processes and technology throughout a bank. Therefore, it would be particularly challenging if cyber-security were managed through its own set of responsibilities, policies and procedures within IT, inconsistent with the overall operational and enterprise-wide risk management framework. To mitigate this challenge, it is necessary to have “advance planning, cooperation and communication between operational, risk, infrastructure and cyber-security teams”.³⁴ Moreover, this requires cyber-risk to be incorporated into the banks’ enterprise-wide risk management framework and governance structure. Like any other bank risk, cyber-risk should be subject to the general risk management principles of risk identification, control, monitoring and mitigation. If necessary to help achieve this, supplemental guidelines may be issued applying or clarifying the application of the general risk management regulations to cyber-risk.
35. **Cyber-security regulations should require banks to develop an effective control and response frameworks for cyber-risk.** The equal focus on a response framework is particularly important given the inevitability of a cyber-attack. The effective execution of banks’ control and response policies throughout the bank should be regularly evaluated. Otherwise, there might be instances where bank-wide cyber policies are applied only in certain areas of the bank. In general, it would be worthwhile to assess whether a sound governance framework and clear accountabilities with regard to cyber-risk are established within the bank.
36. **Any regulation relating to cyber-risk should consider as starting points the existing technical standards on cyber- and information security.** Given the limited availability of resources in the field of cyber-security, particularly in regulatory agencies, existing technical standards on cyber- and information security are useful starting points for regulators. This also avoids having duplicative and/or conflicting expectations when it comes to cyber-security, which will only distract from banks’

³⁴ See Accenture and Chartis (2016).

cyber-security activities as resources will have to be deployed to understand what each differing standard and guideline mean.

37. **A critical element of any regulatory framework is to promote cyber-security awareness among staff.** There is a tendency on the part of both regulators/supervisors and banks to focus too much on technology solutions. Often overlooked is the relevance of the human factor. Policies should encourage banks to develop a framework that enhances awareness among staff about cyber-risk and establishes metrics to measure this awareness. This approach is particularly relevant for smaller jurisdictions with limited resources and threat intelligence capabilities, as well as for dealing with smaller banks.
38. **It is necessary to explore further collaboration with the industry in strengthening banks' cyber-security, and to pursue greater cross-border cooperation and harmonisation of practices.** In some jurisdictions (eg Hong Kong and Singapore), regulators are working closely with the industry in creating or promoting platforms for intelligence-sharing, developing a pool of cyber-security professionals, and establishing guidelines on penetration testing. This could be a model that other jurisdictions could use, especially those with limited regulatory and supervisory resources, smaller banks, or a scarcity of cyber- and information security professionals. Moreover, given the scarcity of cyber-security resources and the cross-border nature of cyber-risk, the need for international harmonisation of regulatory expectations and supervisory cooperation cannot be overemphasised.

References

- Accenture and Chartis (2016): *The convergence of operational risk and cyber security*, February.
- Bank of England (2013): [CBEST framework](#), June.
- Booz Allen Hamilton, Center for Cyber Safety and Education, and ISC (2017): *Global Information Security Workforce Study, US Federal Government Results*, May.
- Center for Internet Security: [CIS Security Controls](#).
- Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (2016): [Guidance on cyber resilience for financial market infrastructures](#), June.
- Council for Registered Ethical Security Testers (2017): [A guide for running an effective penetration testing programme](#), April.
- Deloitte, *Global Risk Management Survey*, 10th edition, 2016.
- Department of Financial Services of New York State (2017): [Cyber-security requirements for financial services companies](#).
- Federal Deposit Insurance Corporation, Federal Reserve Board, and Office of the Comptroller of the Currency (2016): Advance notice of proposed rulemaking: [Enhanced cyber risk management standards](#), October.
- Financial Services Information Sharing and Analysis Center (FS-ISAC), www.fsisac.com.
- Federal Financial Institutions Examination Council (2015): [Cyber security assessment tool](#), June.
- Financial Stability Board (2016): "[Financial Stability Board agrees 2017 workplan](#)", press release, 17 November.
- (2017): *Financial stability implications from fintech: supervisory and regulatory issues that merit authorities' attention*, 27 June.
- Gracie, A (2014): [Managing cyber-risk – the global banking perspective](#), 10 June.
- Hong Kong Monetary Authority (2015a): [Cyber-security risk management](#), September.
- (2015b): [General principles for technology risk management](#), September.
- (2016a): [Cybersecurity fortification initiative](#), May.
- (2016b): [Enhanced competency framework on cybersecurity](#), December.
- (2016c): [Cyber resilience assessment framework \(C-RAF\)](#), December.
- International Association of Insurance Supervisors, issues paper on cyber risk to the insurance sector, August 2016.
- International Organisation for Standardization and the International Electrotechnical Commission (2016): *27000 series – Information security management systems*.
- Central Bank of Ireland (2016): [Cross industry guidance in respect of information technology and cyber-security risks](#), September.
- Kaplan, J, T Bailey, D O'Halloran, A Marcus and C Rezek (2015): *Beyond cybersecurity*, Wiley.
- Lautenschläger, S (2017): "Cyber resilience – A banking supervisor's view", *Statement at the high-level meeting on cyber resilience*, 19 June.

Mee, P and J Morgan (2017): [Deploying a cyber risk strategy: Five key moves beyond regulatory compliance](#), Oliver Wyman.

Monetary Authority of Singapore (2013): [Technology risk management guidelines](#), June.

Monetary Authority of Singapore, notices and circulars on:

- (2014): [Amendment to technology risk management guidelines](#), March.
- (2015a): [Early detection of cyber intrusion](#), August.
- (2015b): [Cyber-security training for the board](#), October.

National Institute of Standards and Technology (2014): [Framework for improving critical infrastructure cybersecurity](#), February.

Netherlands Bank (2017): [Assessment framework for DNB information security examination](#), April.

Raskopf, R, J Prenio, J Crisanto and S Hohl (2016): "Supervisory priorities in non-Basel Committee jurisdictions", *FSI Occasional Paper*, 13 October.

Risk.net (2017): [Top operational risks for 2017](#), 23 January.

Roux, C (2015): [Cybersecurity and cyber risk](#), *Address to the society of actuaries in Ireland risk management conference*, 30 September.

US Government Accountability Office (2015): "Cyber-security, bank and other depository regulators need better data analytics and depository institutions want more usable threat information", Report to Congressional Requesters, July.

US Treasury Department's Financial Crime Enforcement Network (2016): Financial crime enforcement network advisory, 25 October.

US Treasury, [G7 fundamental elements of cybersecurity for the financial sector](#), document endorsed by the G7 finance ministers and central bank governors on 11 October 2016.

World Economic Forum (2017): *Advancing cyber resilience – Principles and tools for boards*, in collaboration with the Boston Consulting Group and Hewlett Packard Enterprise.