FINANCE, COMPETITIVENESS & INNOVATION INSIGHT | FINANCIAL STABILITY & INTEGRITY

Financial Sector's Cybersecurity: Regulations and Supervision

WORLD BANK GROUP

1818 H Street NW
Washington, DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

TABLE OF CONTENTS


Backspace
Home
CYBER
SECURITY
End

ACRONYMS AND ABBREVIATIONS

AICPA	American Institute of Certified Public Accountants
APIs	Application Programming Interfaces
ASIC	Australian Securities and Investment Commission
BaFin	German Federal Financial Supervisory Authority
BCBS	Basel Committee on Banking Supervision
CAPEC	Common Attack Pattern Enumeration and Classification (MITRE Corporation)
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CCI	Commonwealth Cybercrime Initiative
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CPMI	Committee on Payments and Market Infrastructures
CSIRT	Computer Security Incident Response Team
CTO	Commonwealth Telecommunications Organisation
CybOX	Cyber Observable Expression
DDoS	Distributed Denial of Service
EBA	European Banking Authority
ENISA	European Union Agency for Network and Information Security
EU	European Union
FDIC	Federal Deposit Insurance Corporation
FinSAC	Financial Sector Advisory Center
FMI	Financial Market Infrastructure
FRB	Federal Reserve Board
G7	Group of 7
GCSCC	Global Cyber Security Capacity Centre (University of Oxford)
GCSP	Geneva Centre for Security Policy
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission

IOSCO	International Organisation of Securities Commissions
ISAC	Information Sharing Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NYSDFS	New York State Department of Financial Services
OAS	Organization of American States
OCC	Office of the Comptroller of the Currency
OECD	Organisation for Economic Co-operation and Development
PaaS	Platform as a Service
SaaS	Software as a Service
SOC	System and Organization Controls
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Indicator Information
UNCTAD	United Nations Conference on Trade and Development
VCDB	VERIS Community Database (Verizon)
VERIS	Vocabulary for Event Recording and Incident Sharing (Verizon)

ACKNOWLEDGMENTS

The author, Aquiles A. Almansi, is a Lead Financial Sector Specialist, Finance, Competitiveness & Innovation Global Practice at the World Bank Group (WBG). This paper draws on the background work of Dror (2017), Nelson (2017) and Taylor (2017). Detailed comments were received, although not necessarily reflected in this draft, from Dorothee Delort (Senior Financial Sector Specialist), Katia D'Hulster (Lead Financial Sector Specialist), Miquel Dijkman (Lead Financial Sector Specialist), Pasquale Di Benedetta (Senior Financial Sector Specialist), Valeria Salomao Garcia (Senior Financial Sector Specialist), Damodaran Krishnamurti (Lead Financial Sector Specialist), Harish Natarajan (Lead Financial Sector Specialist), Sang Man Park (Senior Financial Sector Specialist) - all of the Finance, Competitiveness & Innovation Global Practice - as well as Iveta Zdravkova Lohovska (Consultant, Information Technology Services, WBG), Sandra Sargent (Senior Operations Officer, Digital Development and Transport, WBG), Zhijun William Zhang (Senior Information Technology Officer, Information Technology Services, WBG), Claus Sengler (European Central Bank), Paul Williams (Bank of England), and Rui Lin Ong (Monetary Authority of Singapore).

A special thanks goes to Aichin Lim Jones (Graphic Designer) for her work on the graphics design of this publication.

INTRODUCTION

According to the Group of 7 (G7) (2016), cybersecurity risks to the global financial system are of critical concern. Attacks on cyberspace, that is, the space between interconnected computers, are "increasing in sophistication, frequency, and persistence, [and] cyber risks are growing more dangerous and diverse, threatening to disrupt our interconnected global financial systems and the institutions that operate and support those systems." Similarly, the International Organisation of Securities Commissions (IOSCO) (2016) has "recognized that cyber risk constitutes a growing and significant threat to the integrity, efficiency and soundness of financial markets worldwide." Compounding the problem, the inexorable trend toward exclusive digital customer interactions increases the financial sector's exposure to cyber risks. In this context, PricewaterhouseCoopers (PwC) (2017) notes that 46 percent of bank customers are already digital-only, compared with 27 percent in 2012. Furthermore, those customers interacting with bank staff continue to shrink, falling from 15 to 10 percent during the same period.

IBM X-Force Research (2017) reveals that the financial services sector was attacked more than any other industry in 2016, with the average financial institution monitored by IBM Security Services experiencing 65 percent more attacks than the average client organization across all industries. Moreover, there was a 29 percent increase in attacks from 2015.[1] In this context, distributed denial of service (DDoS) and ransomware attacks disrupted the provision of financial services in several countries. Money was stolen or confidential data "exfiltrated" (leaked) using other types of malware and "social engineering" tricks.

"Cyber risk," frequently narrowly understood as the occurrence of intentional or malicious "cyber incidents," is just one of the many things that can go wrong in the world of interconnected computers.[2] Information and Communications Technology (ICT) risk, in turn, is traditionally understood as just one class of operational risk, a tradition that could suggest some questionable analogies with other classes of such risk.

To deal with the problem, several leading jurisdictions have issued or proposed detailed laws, regulations or guidelines dealing with cyber risk or, more generally, ICT risk. The World Bank's Financial Sector Advisory Center (FinSAC) (2017) has compiled and continuously updates a digest of this quickly growing body of regulatory and advisory work.

The G7 (2016) sees the following fundamental elements "as the building blocks upon which an entity can design and implement its cybersecurity strategy and operating framework": *governance, risk assessment, monitoring, response, recovery, information sharing, and continuous learning*.

This paper presents the main ideas that can be found widely represented in the FinSAC's Cybersecurity

[1] For detailed analyses and statistics about cyber incidents, see also Symantec (2017), Synoptek (2017), and Verizon (2017a and 2017b).

[2] In addition to intentional incidents, incidents can occur accidentally due to faulty processes, or for purely technical reasons. For a discussion of the many things that can go accidentally wrong due to software complexity, see Somers (2017).

Regulations in the Financial Sector (2017), which coincides with those of the G7's fundamental elements. It also outlines attempts to identify the emerging consensus on practices to implement regulations, as well as on how to supervise their implementation by individual financial institutions.

The paper is organized as follows: Section I briefly presents some different viewpoints with regard to the need for financial institutions to write new regulations. Section II discusses the necessary coordination between financial sector authorities and other state agencies in the regulation and supervision of the sector's ICT systems. Section III presents sample taxonomies (languages) used by different parties to talk about cyber "risks" and share information on cyber "incidents". Sections IV, V, and VI outline, respectively, the responsibilities of the Board, senior management and, if the position exists, the Information Security Officer. Section VII discusses incident response and recovery. Section VIII describes practices regarding tests and simulations. Section IX addresses the increasingly critical issue of outsourcing. Section X presents sample guidelines for supervisors, and section XI contains concluding remarks.

The mandatory or suggested practices identified in this paper are those of primary interest for the financial sector authorities in charge of regulating and/or supervising licensed banking and non-banking institutions. As more dimensions of the provision of financial services migrate to the space of interconnected computers (or "cyberspace"), other state and regional agencies — such as European Union Agency for Network and Information Security (ENISA), and national security agencies in some jurisdictions — will be regulating how operations are to be conducted in their respective domains. This implies that financial institutions in some jurisdictions will have to abide by a growing number of regulations pertaining to technical ICT matters beyond the regulatory perimeter of the financial sector authorities, such as encryption protocols, application programming interfaces (APIs), or authentication mechanisms. These are outside the scope of this paper.

While the provisional findings of this work are significantly enhanced by the FSB stocktaking of existing regulations and supervisory practices in G20 jurisdictions presented last October, financial sector authorities from World Bank client countries, in search of guidance on whether and how to regulate and supervise cyber risk management in institutions subject to their jurisdiction, may find the main ideas here described a good starting point.

I. ARE CYBER-SPECIFIC REGULATIONS NECESSARY?

Crisanto and Prenio (2017) note that there are differing institutional views about whether and how to regulate cyber risks. "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 regulations relating to technology and/or operational risk. The other view is that [a] regulatory structure is needed to deal with the unique nature of cyber risk, and given the growing threats resulting from an increasingly digitized financial sector."

Commenting on the United States Federal Reserve Board/ Office of the Comptroller of the Currency/ Federal Deposit Insurance Corporation (FRB/OCC/ FDIC) advanced notice of proposed rulemaking on enhanced cyber risk management standards (2016), Promontory (2017) notes that a "rulemaking that imposed overlapping new cybersecurity standards on top of the multiple existing standards, without any empirical analysis of actual effects, would be counterproductive. Rather than improving cybersecurity, such a rulemaking would divert to unproductive compliance processes the very resources that covered entities could otherwise devote to securing operations." In this context, Crisanto and Prenio (2017) note that 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 cybersecurity."

Promontory points out the multiple, overlapping, international cybersecurity standards such as the International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27000 (2016), ISO/IEC-27001 (2005), ISO/ IEC-27002 (2013), the System and Organization Controls (SOC) for Cybersecurity of the American Institute of Certified Public Accountants (AICPA)[3], frameworks such as the one from the National Institute of Standards and Technology (NIST) (2017 and 2014), as well as guidelines like those of the Committee on Payments and Market Infrastructures (CPMI-IOSCO) (2016), and regulations on operational risk management in most national jurisdictions..

Management failures occur because too many people still see cybersecurity as a technical matter, reserved for the exclusive domain of information technology (IT) specialists. As Crisanto and Prenio (2017) suggest, regulations that actually deal mostly with corporate governance matters make cybersecurity more visible to Boards and Management, thereby providing stronger incentives to them to take responsibility for it.

Traditional ways of thinking about operational risk, incorporated in some regulations on cyber risk, may not be fully adequate to deal with the new reality. Principle 25 of the Basel Committee on Banking Supervision (BCBS) (2012), for example, includes among its essential criteria the provision that "The supervisor requires banks' strategies, policies and processes for the management of operational risk (*including the banks' risk appetite for operational risk*) to be approved and regularly reviewed by the banks' Boards." However, given the systemic magnitude of cybersecurity risk derived from the

[3] http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx

system's interconnected nature, it is unclear why the degree of cyber risk taken by an individual institution should depend in any sense on the Board's risk "appetite" for operational risk. The presence of negative externalities would suggest setting minimum standards regardless of such "appetite," or any other subjective consideration.[4]

Technical complexity (in the number of potential entry points for an attacker and in the diversity of services), the capacity to deal with it, and the potential systemic impact of cyber incidents are likely to be proportional to the size of the financial institution. As such, some of the emerging guidelines and regulations fully apply to large institutions only.[5] Since an interconnected system is as strong as the weakest of its nodes, some jurisdictions may well choose to consider subjecting all interconnected institutions to the same minimum cybersecurity standards, regardless of size.

[4] For example, the average delay in departures, and the proportion of luggage lost, could indeed be left to an airline's "risk appetite," but the frequency of crashes probably should not.

[5] Standards set forth by the FRB-OCC-FDIC (2016), for example, would apply to all U.S. bank holding companies with total consolidated assets of $50 billion or more.

II. COORDINATION AMONG AUTHORITIES

"...each distinct aspect of cybersecurity (...cyber crime, intelligence, military issues, Internet governance, or national crisis management) operates in its own silo, belonging, for instance, to a specific government department or ministry. Each of these silos has its own technical realities, policy solutions, and even philosophies."

Klimburg (2017)

Principle 2 of the BCBS (2012) requires the bank supervisor to possess "operational independence", and the first essential criteria for the observance of such a principle requires that "no government or industry interference ... compromises the operational independence of the supervisor," and that the "supervisor has full discretion to take any supervisory actions or decisions on banks and banking groups under its supervision." These requirements are fully consistent with the supervision of managerial behaviors. However, the regulation and supervision of ICT risks, as well as the response to incidents, may require the intervention of other state agencies.

Many countries have already published national cybersecurity strategies, frequently identifying the state agencies in charge of setting minimum standards and responding to a cyber incident. References to bank security can already be found in the following country strategies: Australia, Austria, Bangladesh, Brunei Darussalam, Canada, China, Colombia, the Arab Republic of Egypt, France, Ghana, Ireland, Italy, Japan, Jordan, Kenya, Malaysia, Micronesia, Morocco, the Netherlands, New Zealand, Nigeria, Norway, Poland, Qatar, the Russian Federation, Saudi Arabia, Singapore, Slovakia, Slovenia, Sweden, Switzerland, the United Kingdom (UK), and the United States (US).[6] National cybersecurity strategies and legal frameworks should clearly specify the respective responsibilities of the financial sector and other authorities, such as national security agencies. Without such clarity, jurisdictional conflicts are bound to arise when issuing new cybersecurity regulations or, even worse, when handling cyber incidents in the financial sector.[7]

A new reference guide is being developed by a host of organizations to serve as a single source to guide countries in developing their own national cybersecurity strategies. This guide should also help financial sector authorities better understand the nature of the institutional structure required to deal with cybersecurity. It is currently being prepared by the International Telecommunication Union (ITU), a United Nations agency, in partnership with the Commonwealth Cybercrime Initiative (CCI), the Commonwealth Telecommunications Organisation (CTO), ENISA, the Geneva Centre for Security Policy (GCSP), the University of Oxford's Global Cyber Security Capacity Centre (GCSCC), Intellium, Microsoft, the North Atlantic Treaty Organization (NATO)'s Cooperative Cyber Defence Centre of Excellence (CCDCOE), the Organisation for Economic Co-operation

[6] http://www.itu.int/en/ITU-D/Cybersecurity

[7] An important example of a legal framework that clarifies the roles of different state agencies is EU (2016), naturally including cross-border considerations in the European Union

and Development (OECD), the Organization of American States (OAS), the Potomac Institute, RAND Europe, the United Nations Conference on Trade and Development (UNCTAD) and the World Bank.

III. MANDATORY REPORTING AND INFORMATION SHARING

Previous sections assume a common understanding of what is meant by words such as "cyber", "risks" and "incidents," as used by the G7 (2016), the International Organisation of Securities Commissions (IOSCO) (2016) and IBM (2017), among others. To understand how different organizations utilize these terms requires knowing their respective "taxonomies" (languages) is required. All stakeholders need precise, common languages to share information, either of the mandatory kind, between supervisory institutions and authorities or, to prevent the spread of cyber incidents, voluntarily with other potentially affected entities.

Taxonomies are languages or conventions for information sharing, and there are many of them. For instance, ICT specialists frequently work with MITRE Corporation's "Common Attack Pattern Enumeration and Classification" (CAPEC), a "comprehensive dictionary and classification taxonomy of known attacks that can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses".[8] Regarding *mechanisms of attack*, CAPEC identifies 118 different mechanisms to collect and analyze information; 152 to inject unexpected items;156 to engage in deceptive interactions; 172 to manipulate timing and state; 210 to abuse existing functionality; 223 that employ probabilistic techniques; 225 that subvert access control; 255 that manipulate data structures; and 262 that manipulate system resources. Regarding *domains of attack*, CAPEC identifies 403 different types of social engineering; 437 on the supply chain; 512 on communications; 513 on software; 514 on physical security; and 515 on hardware.

Verizon offers the "Vocabulary for Event Recording and Incident Sharing" (VERIS) to help organizations "collect and share useful incident-related information anonymously and responsibly."[9]

VERIS is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner, namely: the "who" (threat actors), the "what" (victim assets), the "why" (threat motives), and the "how" (threat actions) of each cybersecurity incident.[10]. The VERIS Community Database (VCDB) is an open and free repository of publicly-reported security incidents in VERIS format.[11]

Another taxonomy available for the automated sharing (primarily among computer systems, not among people!) of threat information in standardized format was originally developed by the US Department of Homeland Security. It is currently maintained by an open community[12], and is composed of the freely available Trusted Automated Exchange of Indicator Information (TAXII), the Cyber Observable Expression (CybOX), and the Structured Threat Information Expression (STIX).

Apart from highly specialized units in financial supervisory agencies, none of these taxonomies are likely to be very useful for information sharing among financial sector authorities, or between them and the Boards and Senior Management of

[8] CAPEC: Common Attack Pattern Enumeration and Classification—A Community Resource for Identifying and Understanding Attacks, https://capec.mitre.org/.
[9] "Veris: The Vocabulary for Event Recording and Incident Sharing" at: http://veriscommunity.net.
[10] "Vocabulary for Event Recording and Incident Sharing" at: https://github.com/vz-risk/veris.
[11] VCDB raw data is available at: https://github.com/vz-risk/VCDB
[12] Oasis Cyber Threat Intelligence" at: https://wiki.oasis-open.org/cti/.

supervised institutions. In this context, the European Banking Authority (EBA) (2017), for example, asks European bank supervisors to map identified ICT risks into the following five risk categories:

- **Availability and continuity risk:** the risk that the performance and availability of systems and data are adversely impacted, including the inability to timely recover due to a failure of hardware or software, management weaknesses, or any other event.

- **Data integrity risk:** the risk that data stored and processed are incomplete, inaccurate or inconsistent across different systems.

- **Change risk:** the risk arising from the inability of the institution to manage system changes in a timely and controlled manner.

- **Outsourcing risk:** the risk that engaging a third party, or another group entity (intra-group outsourcing), to provide systems or related services, adversely impacts the institution's performance and risk management.

- **Security risk:** the risk of unauthorized access to systems from within or outside the institution.

Data integrity, and services availability and continuity are some of the dimensions that may, for many different reasons, go awry with the ICT systems of a financial institution. In other words, *services can be disrupted and/or data compromised*. Physical and logical ("bugs") can impact ICT systems, and institutions can fail to properly manage the constantly changing state of their ICT systems,[13], and/or the external providers of outsourced services. Additionally, ICT systems can fail because of security reasons, that is, when someone from inside or outside the institution intentionally does something that disrupts services or affects data integrity.

The EBA's first four "ICT risks" remain, at least conceptually, reasonably well defined over time, but "security" risks keep mutating. As illustrated by the CAPEC taxonomy, there are literally thousands of ways (by combining different "domains" and "mechanisms" of attack) that a financial institution's ICT systems can be compromised. Attacks can occur without penetrating ICT systems; or by penetrating them with or without hacking them; by insiders or a variety of outsiders; with or without "social engineering"; with or without physical access to them — and many more ways yet to be discovered.

Once an incident has affected the ICT systems of a supervised institution, EBA's taxonomy provides a language to communicate possible answers as to what has happened (services disrupted and/or data integrity affected?) and why it has happened (autonomous system malfunction, or inadequate management of own and/or third-party systems, and/or malicious third-party intervention?). Although only some supervisory agencies may have the internal capacity to make productive use of strictly technical information, as described for example by the taxonomies of CAPEC or TAXII-CybOX-STIX, all supervisors need a taxonomy to describe the impacts of an incident. Once again, EBA offers a helpful taxonomy of the possible *impacts* of an incident, as follows:[14]

- **Financial impact** including (but not limited to) loss of funds or assets, potential customer compensation, legal and remediation costs, contractual damages, lost revenue;

- **Business disruption**, considering (but not limited to) the criticality of the financial services affected; the number of customers and/or branches and employees potentially affected;

- **Reputational impact** based on the criticality of the banking service or operational activity

[13] The state of ICT systems keeps changing because, in addition to new applications or new features in existing ones, they constantly undergo security updates. Any of these changes can break a system at any time.

[14] To understand the essentially linguistic (conventional) role of all taxonomies, these impacts are what other parties would perhaps prefer to call the risks associated to an ICT incident.

affected (e.g., theft of customer data); the external profile/visibility of the ICT systems and services affected (e.g. mobile or on-line banking systems, point of sale, ATMs or payment systems);

- **Regulatory impact,** including the potential for public censure by the regulator, fines or even variation of permissions; and

- **Strategic impact**, if strategic products or business plans are compromised or stolen.

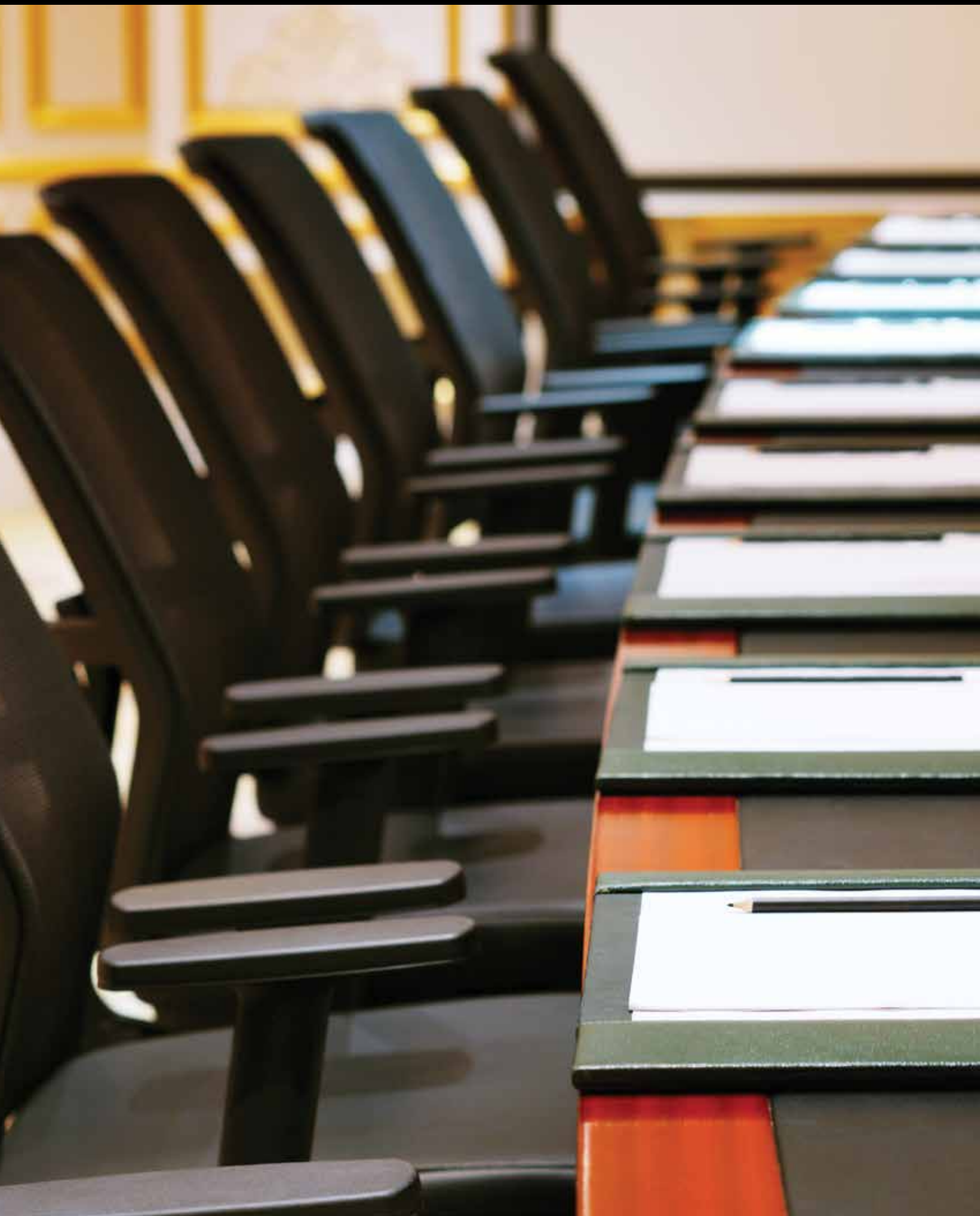
Supervisory taxonomies facilitate information sharing among supervisors, and between them and supervised institutions. Given the potential *regulatory impact*, however, supervised institutions have limited incentives to voluntarily report incidents. Consequently, some jurisdictions make such reporting mandatory. The European Union (EU) (2016), for example, regulates the mandatory notification of a *significant incident* as follows:

> "Banking corporations shall notify, without undue delay, the competent authority of incidents having a significant impact on the continuity of the essential services they provide, or in case that there is a reasonable likelihood of materially harming business operations. Notifications shall include information enabling the competent authority to determine any *impact of the incident*. Notification shall not make the notifying party subject to increased liability." Furthermore, it specifies the following parameters as determining the magnitude of the impact: "(a) the number of users affected by the disruption of the essential service; (b) the duration of the incident; and (c) the geographical spread with regard to the area affected by the incident."

It is important to note that in addition to establishing a mandatory reporting requirement, the EU (2016) states its precise purpose (*to enable the competent authority to determine any impact of the incident*), and it also defines how to account for such an impact. Without stating the precise purpose of the notification, in many countries the supervisory authority could easily become liable for what it does — or does not do — in responding to an incident. As suggested in section II, responding to an incident is likely to eventually become the responsibility of other state agencies, such as a Computer Emergency Response Team (CERT) or a Computer Security Incident Response Team (CSIRT), possibly associated with a national security agency. This in turn may also require mandatory reporting, with a different taxonomy.[15]

Reporting on the impact of an incident to the supervisory authority should not be confused with the voluntarily sharing of technical information that could help other institutions take preventive actions. To deal with the limited incentive to reveal problems there are different initiatives, either private or in public-private partnerships, to voluntarily share information about incidents on an anonymized basis. Crucially, this can be done in a language that facilitates the taking of immediate preventive actions. For example, one success story concerns the Information Sharing Analysis Centers (ISACs) in the United States, which includes a financial services ISAC automatically sharing information among members utilizing the TAXII-CybOX-STIX taxonomy.

[15] Establishing a financial sector CERT or CSIRT as a dependency of the Central Bank is not unthinkable, but in many jurisdictions, it could potentially create significant contingent liabilities.



IV. RESPONSIBILITIES OF THE BOARD

"...we seem conceptually trapped in thinking of the new challenges of cyberspace as being purely technical, instead of being very much human."

Klimburg (2017)

Principle 25 of BCBS (2012) requires supervisors to verify that a bank's strategies, policies and processes for the management of operational risk are approved and regularly reviewed by the Board — and that the Board oversees their effective implementation. Consistent with this general principle, regulations and guidelines specifically dealing with cyber risk (for example, the Australian Securities and Investment Commission [ASIC] (2015); CPMI-IOSCO (2016); FRB-OCC-FDIC (2016); Ireland (2016); and Israel (2015)) typically require that the Board of supervised institutions: (i) approve a written ICT strategy aligned with the institution's overall business strategy; (ii) approve a comprehensive ICT risk management framework; and iii) oversee senior management's effective implementation of both the strategy and risk management framework.

In several regulatory documents, the Board's role is expected to go well beyond that of adopting strategies and frameworks to encompass the oversight of their effective implementation. Ireland (2016), for example, requires the Board to "receive reports on significant cyber incidents", and so does Israel (2015). ASIC (2015) not only asks to "review the level of Board and Senior Management oversight of cyber risks," but also "how frequently risks are updated."

The Central Bank of Ireland (2016) requires the Board to receive "updates on the scenarios considered and the development and testing of disaster recovery and business continuity plans." and to understand "what the objectives of these are in terms of maintaining availability of critical IT systems and business operations." Furthermore, it expects the Board (as a whole) and Senior Management to "possess sufficient *knowledge and understanding* of the IT- related risks facing the firm, and [to] take steps to ensure that these risks are well understood and properly managed throughout the firm." They should also be able to demonstrate to supervisors that these steps have been taken.

The findings of the "Bridging the Technology Gap in Financial Services Boardrooms' report by Accenture (2015) suggest that the required *knowledge and understanding* are still rather scarce. According to that report, "only 6 percent of Board members and 3 percent of CEOs at the world's largest banks have professional technology experience. In addition, 43 percent of the banks have no Board members, and nearly 30 percent have only one Board member, with professional technology experience." Ho (2015) has an answer for such a knowledge gap: the Monetary Authority of Singapore "expects that the Board be regularly apprised on salient technology and cyber risk developments." Furthermore, financial institutions "should have in place a comprehensive technology risk and cybersecurity training program for the Board. Such a program may comprise periodic briefings conducted by in-house cyber security professionals or external specialists. The goal is to help equip the Board with the requisite knowledge to competently exercise its oversight function, and appraise the adequacy and effectiveness of the financial institution's overall cyber resilience program."

V. RESPONSIBILITIES OF SENIOR MANAGEMENT

The Bank of Israel (2015) serves as a representative example of the duties of an institution's senior management regarding cybersecurity regulations and guidelines, as follows:

- Creating the cyber risk management framework and overseeing its implementation;
- Formulating the corporate cyber defense policy;
- Implementing and consistently maintaining the cyber risk, including allocating sufficient resources;
- Monitoring the effectiveness of the cyber defense, and coordinating with internal and external risk management entities;
- Receiving periodic reports on cyber threats;
- Receiving periodic reports on relevant, internal and external cyber incidents and their implications;
- Discussing the operative implications of cyber risks, and providing guidance and control over the implementation of any required changes.

Senior management needs to receive periodic reports on cyber threats and incidents to design the appropriate cyber risk management framework and cyber defense policy, very much as the Board needs to receive the same information to understand and approve such framework and policy, and to oversee their effective implementation by Senior Management. Neither in the case of the Board nor that of Senior Management, however, regulations make clear the point of receiving reports on cyber incidents beyond that of informing eventually necessary adjustments in strategies, policies, risk management frameworks, disaster recovery and business continuity plans.

Dealing with cyber incidents may require taking *business decisions* that would normally not make sense to delegate to ICT staff. For example, if it is found that unknown malware has compromised a critical system, who is to be held personally responsible for taking the decision to shut down the system until the problem is resolved or, alternatively, continue providing the system's services while ICT staff work to neutralize it? This type of business decision requires choosing between a (financially, reputationally, regulatorily) costly disruption of services now, and the possibility of a catastrophic disruption later. Such a problem would seem to fall under the purview of Senior Management and/or executive members of the Board. In this regard, financial sector regulations on cyber risk do not explicitly delineate how such critical decisions are to be made regarding the responsibilities of Senior Management. As discussed in section VII, only those regulations dealing with incident response require an explicit assignment of responsibilities in the *incident response* plan.


Protecte

VI. INFORMATION SECURITY OFFICER

As noted in sections IV and V, existing regulations assign concrete responsibilities regarding ICT security/cybersecurity to the Board and Senior Management. Although less common, some regulations already require the appointment of an Information Security Officer, Chief Information Security Officer (CISO), or Chief Cyber Defense Officer. The National Institute of Standards and Technology (NIST) (2017) framework assumes its existence, and the New York State Department of Financial Services (NYSDFS) (2017) requires a CISO. However, subject to certain conditions, the latter allows for the hiring of an independent contractor.

Israel (2015), Korea (2016) and the German Federal Financial Supervisory Authority (BaFin) (2017) provide similar job descriptions for the CISO. Israel (2015) states that this officer "shall report to a senior executive of the banking corporation, and shall officially be given the authority to influence any decisions that affect the banking corporation's exposure to cyber risks." As this entails helping to manage trade-offs between business and cybersecurity objectives, all these regulations emphasize the need to prevent conflicts of interest. BaFin (2017), for example, requires separating this function from the internal audit and the areas responsible for the operation and further development of the IT system.[16], as well as providing it with adequate resources.

Another important role for the CISO is to lead the institution's continuous learning on cybersecurity. Israel (2015) asks the CISO to "promote cyber threats awareness and provide training on mitigation processes across the banking corporation including employees, suppliers, partners and customers." Korea (2016) expects the CISO to "develop an educational program to strengthen the ability of executives and employees to deal with information security, and to formulate and execute an annual educational plan." Directly related to this educational role, Israel (2015) also requires the CISO to "initiate and execute cyber exercises."

Finally, BaFin (2017) creates the obligation for employees of the institution, as well as IT service providers, to provide immediate and comprehensive information to the Information Security Officer on all known IT-related issues affecting the institution. Requiring this reporting from IT service providers is related to the handling of outsourcing, as discussed in section IX.

[16] The Chief Information O could, for example, be reluctant to approve IT security features that hinder project delivery.

VII. INCIDENT RESPONSE

CPMI-IOSCO (2016) states that a "Financial Market Infrastructure (FMI) should involve its Board and Senior Management appropriately, for example, as part of crisis management teams." However, financial regulations on cybersecurity typically do not explicitly list incident response responsibilities for members of the Board and/or Senior Management. These responsibilities are expected to be assigned in the institution's *incident response plan*. EBA (2017), for example, requires "a documented incident management and escalation process, that also provides guidance on the different incident management and escalation roles and responsibilities, the members of the crisis committee(s) and the chain of command in case of emergency."

NYSDFS (2017) details the required content of their incident response plan as follows:

- The internal processes for responding to a cybersecurity event;
- The goals of the incident response plan;
- The definition of clear roles, responsibilities and levels of decision-making authority;
- External and internal communications and information sharing;
- Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
- Documentation and reporting regarding Cybersecurity Events and related incident response activities;
- The evaluation and revision, as necessary, of the incident response plan following a cybersecurity event.

Although assigning decision-making responsibilities is essential, doing so only in the context of a plan may be counterproductive if such a plan is not sufficiently general in nature. If the concept of a "plan" is narrowly understood as detailing well-defined steps to deal with well-defined contingencies, such as fires or earthquakes, it may be unhelpful in the constantly evolving and unpredictable realm of cyber incidents.[17]

[17] In a Cyber Crisis Simulation Exercise (CCSE) delivered by the World Bank there were two groups composed of senior operational risk staff representing, respectively, the Senior Management teams of two banks facing severe cyber incidents. One of the teams assessed the situation as described in the scenario and responded accordingly; the other had problems because it did not have a "plan" for it!


INTERNET
PASSWORD
CODE
DATA
INTERNET
SECURE
6E78BC9

VIII. TESTS AND SIMULATIONS

Cybersecurity regulations and guidelines typically require or suggest regular tests and simulations of incident response capabilities. For example, EBA (2017) instructs supervisors to verify whether a supervised institution's risk management framework "tests ICT availability and continuity solutions, against a range of realistic scenarios including cyberattacks and tests of back-ups for critical software and data which:

- are planned, formalized and documented, and the test results used to strengthen the effectiveness of the ICT availability and continuity solutions;
- include stakeholders and functions within the organization, such as business line management including business continuity, incident and crisis response teams, as well as relevant external stakeholders in the ecosystem;
- include management; Board and Senior Management are appropriately involved in … a *crisis management team*… and are informed of test results."

The typical technical test, *penetration testing*, involves hiring "white hat" hackers who attempt to penetrate the institution's ICT systems using different techniques, from "sniffing" the network for open ports, to different forms of "social engineering".[18] Such testing is required or suggested by multiple regulations and guidelines, such as: CBEST (2016), Crisanto and Prenio (2017), the United Kingdom's Department for Digital, Culture, Media and Sport (DCMS) (2016), EBA (2017), FRB-OCC-FDIC (2016), IOSCO (2016), Ireland (2016), NIST (2017) and Malaysia (2016).

Crisis simulation exercises involving key stakeholders, such as Board Members and Senior Management, are intended as "learning-by-doing" exercises, that is, practicing information sharing and coordination among decision makers.[19]

[18] This could involve tricking staff with emails appearing to come from their bosses with unusual requests, clicking on poisoned hyperlinks, or downloading attachments containing malware.

[19] Major banks have been doing these exercises for years. The World Bank has delivered more than 30 crisis simulations exercises for financial sector authorities since 2008, with scenarios frequently including some and, occasionally only, cyber incidents as triggers of financial instability.

IX. OUTSOURCING

Financial institutions increasingly rely on diverse IT service providers. Cloud services, in particular, are evolving from providing just "infrastructure as a service" (IaaS) to "platform as a service" (PaaS), and even to "software as a service" (SaaS).

Outsourcing has traditionally been an important challenge in operational risk management, and current cybersecurity regulations and guidelines contain the usual expectations about an institution's capacity to manage it. EBA (2017), for example, expects an institution to have "an effective framework in place for identifying, understanding and measuring ICT outsourcing risk, and in particular, controls and a control environment in place for mitigating material outsourced ICT services that are commensurate with the size, activities and the ICT risk profile of the institution." A key expectation is that the supervisor assesses the institution's capacity to "review the ICT risk management policies and the ICT *controls and control environment of the service provider* to ensure that they meet the institution's internal risk management objectives and risk appetite."

Institutions of all sizes and risk profiles need to rely, at least partially, on proprietary (hence closed-source) software applications developed by third parties, which are in turn normally built on top of many different libraries developed by additional third parties entirely unknown to the bank. Consequently, it may not be particularly realistic to expect supervised institutions to be able review the ICT controls of so many (including unknown) developers. However, "cloud computing" has freed the banks, and many other organizations (partly including the World Bank), of owning and securely maintaining a data center. The largest providers of cloud services in the US and other countries are key technology players such as Amazon, Google, HP, IBM, and Microsoft. It is unclear whether an individual bank, including the largest institutions, could meaningfully review the "ICT controls and control environment" of such service providers. These are also typically outside the regulatory perimeter, and frequently outside the national jurisdiction, of financial sector authorities.

Given the apparently irreversible migration to the cloud by most financial sector institutions, two interesting questions arise. First, who should be in charge of regulating and supervising cloud providers? Second, to what extent does the reliance on the increasingly homogeneous services of cloud providers contribute to systemic risk?


EQUIREMENTS
TRANSPAR
COMPLIANCE
STANDARDS
REGULATI
LAW

X. SUPERVISION

In assessing the quality of Board and Senior Management oversight of IT risks, Ireland (2016) offers a clear example of the inadequate managerial practices that skillful supervisors can uncover in the field, including the following ones directly related to sections IV, V and VII:

- Insufficient alignment between the IT and business strategies.
- The quality and/or frequency of IT-related reporting to the Board is highly variable and, in many cases, deficient.
- In general, the board and Senior Management are not sufficiently informed about the operational risk profile of the firm, including IT and cybersecurity risks.
- Inadequate and/or infrequent testing of disaster recovery and business continuity plans and failure to inform the Board of the outcomes of this testing.

Although supervisory practices are not as publicly available as the regulatory texts that supervisors must enforce, EBA (2017) offers detailed, probably quite representative, guidelines. Its general provisions, some of which touch on themes discussed in this paper, are as follows:

- "...the frequency, scope and intensity of the supervisory review of an institution, and also the supervisory expectations of the standards the institution is expected to meet ...should be proportionate to the size, structure and operational environment of the institution as well as the nature, scale and complexity of the institution's activities."
- "...the increasing reliance on outsourced ICT services and third-party products, often in the form of diverse packaged solutions", results "in manifold dependencies [,] … potential constraints and new concentration risks."
- "... authorities should use existing and available documentation (for example, relevant reports and other documents, meetings with risk management, on-site inspection findings) to inform their assessment."
- "... authorities may exclude some of the ICT risks included in the taxonomy if not pertinent to their assessment."

It follows from these general provisions that the key consideration that sets current perceptions about the challenges of ICT risk supervision apart from those of more conventional supervisory tasks is the increasing reliance on outsourced ICT services. Consequently, the wisdom of EBA's representative guidelines critically depends on those perceptions.[20] The guidelines cover the following matters in detail:

- ICT governance and strategy, including: general principles; development of the ICT strategy; and implementation of the ICT strategy, internal governance, and risk management.

[20] Can each and every financial institution, including the largest and most sophisticated ones, realistically be expected to "review" the ICT controls and control environment of each and every one of the developers writing the code that runs its ICT systems to ensure that no "backdoor" or malware is inserted? (Windows 10 alone currently has more than 40 million lines of proprietary, closed-source code) Can each and every financial institution meaningfully review the ICT controls and control environment of major "cloud" providers, such as Amazon, Google, HP, IBM, and Microsoft? Would an in-house data center (running millions of lines of unknown code written by unknown developers) be easier for an institution to review and for authorities to supervise?

- ICT risk exposures and controls, including: general considerations; identification of material ICT risks; and assessment of the controls to mitigate material ICT risks.

Given the current state of the global labor market for IT specialists, finding and retaining technically qualified staff to assess an institution's ICT strategy, and its exposures and controls, are daunting tasks for most jurisdictions, including major ones. This is yet another reason to reflect on the allocation of regulatory and supervisory responsibilities among state agencies, as discussed in section II.

XI. CONCLUDING REMARKS

The increasing reliance on ICT technology will require a careful distribution of regulatory and supervisory powers between financial sector authorities and other state agencies. Without a clear legal framework, jurisdictional conflicts are inevitably bound to arise in many countries.

Due to the contagion potential derived from the interconnected nature of contemporary financial infrastructure, traditional concepts such as "proportionality" in regulatory requirements and supervisory attention, and "risk appetite for operational risk," may have to be revised. An interconnected system is as strong as its weakest link. Hence, it may be necessary to set minimum cybersecurity standards for all institutions, independently of other dimensions of their systemic importance.

Comparing the responsibilities of the Board and Senior Management, as described in sections IV and V, with the detailed questions that supervisors following guidelines such as those of EBA (2017) would be inclined to ask, the findings of Ireland (2016) are not surprising. Furthermore, Accenture (2015) reveals that most Board members, even those from the largest banks in the world, would likely have trouble offering satisfactory answers. In some legal frameworks, dealing with this problem may require writing substantially more detailed regulations regarding the responsibilities of the Board and Senior Management.

Increasing the outsourcing of ICT services is an irreversible trend, which can perhaps decrease the ICT risk of individual institutions. However, it might also contribute to heightened systemic risk.

Although some regulations explicitly require cybersecurity training for the Board, Senior Management, and employees, surprisingly there are no widespread references yet to training the growing number of digital customers of financial services.


REFERENCES
ENTER

REFERENCES

Accenture. 2015. *Bridging the Technology Gap in Financial Services Boardrooms.*

ASIC (Australian Securities & Investments Commission). 2015. *Cyber Resilience: Health Check.* Report 429.

BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht– German Federal Financial Supervisory Authority). 2017. *Bankaufsichtliche Anforderungen an die IT (BAIT)*. Konsultation.

BCBS (Basel Committee on Banking Supervision). 2012. *Core Principles for Effective Banking Supervision.*

CBEST (California Basic Educational Skills Test). 2016. *CBEST Intelligence-Led Testing, Implementation Guide.*

CPMI-IOSCO (Committee on Payments and Market Infrastructures- International Organisation of Securities Commissions). 2016. *Guidance on cyber resilience for financial market infrastructures*. Bank for International Settlements and International Organization of Securities Commissions.

Crisanto, Juan Carlos and Jeremy Prenio. 2017. *Regulatory approaches to enhance banks' cyber-security frameworks*. FSI Insights on Policy Implementation No 2. Financial Stability Institute, Bank of International Settlements.

DCMS (UK Department for Digital, Culture, Media and Sport). 2016. *Cyber security regulation and incentives review.*

Dror, Ishai. 2017). *Cybersecurity Regulation in the Financial Sector. Key concepts in existing and proposed regulations*. Unpublished manuscript.

EBA (European Banking Authority. 2017. *Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP)*.

EU (European Union), 2016. *Directive 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union - NIS.*

FinSAC (World Bank's Financial Sector Advisory Center). 2017. *Cybersecurity*

Regulations in the Financial Sector: A Digest. Vienna, Austria: The World Bank-FinSAC.

FRB-OCC-FDIC (Federal Reserve Board- Office of the Comptroller of the Currency- Federal Deposit Insurance Corporation). 2016. *Advance Notice of Proposed Rulemaking (ANPR) Regarding Enhanced Cyber Risk Management Standards for Large and Interconnected Entities*. United States: Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation.

G7 (Group of 7). 2016. *Fundamental Elements of Cybersecurity for the Financial Sector.*

Ho, Hern Shin. 2015. Circular No. SRD TR 03/2015. *Monetary Authority of Singapore (MAS).*

IBM (International Business Machines). 2017. *Security trends in the financial services sector.* IBM X-Force Research.

IOSCO (International Organisation of Securities Commissions). 2016. *Cyber Security in Securities Markets – An International Perspective.*

Ireland, Central Bank of. 2016. *Central Bank Guidance on IT and Cyber SecurityRisks.*

ISO/IEC (International Organization for Standardization/ International Electrotechnical Commission)-27000. 2016. *Standard 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

_____. 27001. 2005. *Standard 27001: Requirements on Information technology – Security techniques – Information security management systems.*

_____. 27002. 2013. *Standard 27002: Information Technology – Security Techniques – Code of Practice for Information Security Controls. Second edition.*

Israel, Bank of. 2015. *Cyber Defense Management Directive.*

Klimburg, Alexander. 2017. *The Darkening Web. The War for Cyberspace. Penguin Press: New York.*

Korea. 2016. *Regulation on Supervision of Electronic Financial Transactions.*

Malaysia, Securities Commission. 2016. *Guidelines on Management of Cyber Risk SC-GL/2-2016.*

Nelson, Winston. 2017. *Taxonomy of ICT Risks.* Unpublished manuscript.

NIST (National Institute of Standards and Technology). 2017. *Cybersecurity Workforce Framework.* NIST Special Publication 800181.

_____. 2014. *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.0.

NYSDFS (New York State Department of Financial Services). 2017. *Cybersecurity Requirements for Financial Services Companies.*

Promontory. 2017. *Comments to ANPR on Enhanced Cyber Risk Management Standards*. February 15. Promontory Interfinancial Network.

PwC (Pricewaterhouse Coopers). 2017. *Digital Banking Survey*.

Somers, James. 2017. "The Coming Software Apocalypse." *The Atlantic Magazine*. September 26.

Symantec. 2017. *Internet Security Threat Report*.

Synoptek_____. 2017. *Cybersecurity Outlook for Financial Services Organizations.*

Taylor, Charles. 2017. *Cyber Preparedness for Financial Regulators*. Unpublished manuscript.

Verizon. 2017a. *Data Breach Investigations Report.* 10th Edition.

_____.2017b. *Data Breach Digest.*


WORLD BANK GROUP