December 10, 2018

Basel Committee on Banking Supervision Publishes Report on Cyber-Resilience Practices

SUMMARY

On December 4, 2018, the Basel Committee on Banking Supervision (the "Basel Committee") published a report entitled "Cyber-resilience: Range of practices,"[1] which broadly surveys and compares the range of bank, regulatory and supervisory cyber-resilience practices across jurisdictions. According to the Basel Committee, the report is intended to help banks and supervisors "navigate the regulatory environment and will serve as a useful input for identifying areas where further policy work by the Committee may be warranted."

The Basel Committee organizes their review of cyber-resilience into four broad categories: (1) governance arrangements and culture; (2) approaches to cyber-risk management, testing, and incident response and recovery; (3) communications and information-sharing; and (4) expectations and practices related to interconnections with third-party service providers.

BACKGROUND

In response to the proliferation of cybersecurity threats and incidents, the Basel Committee developed a report focused on cyber-resilience, defined by the Financial Stability Board (FSB) as "the ability of an organization to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents."

The report is based on responses from the members of the Operational Resilience Working Group (ORG), a sub-committee established by the Basel Committee, to a survey prepared by the FSB in April 2017. In addition, the report reflects insights from ORG members and communications with industry

stakeholders, including banks, utility and technology service providers, consultancies and associations involved in cybersecurity matters.

DISCUSSION

1. Key Findings.

Within the report, the Basel Committee identifies 10 key findings:

- ***General landscape.*** The Basel Committee found that most supervisors leverage previously adopted national or international standards for cyber-resilience, such as the NIST and ISO frameworks. Despite general alignment at a high level, however, technical specifications and supervisory practices vary across jurisdictions, "result[ing] in a complex and somewhat fragmented international regulatory landscape."
- ***Strategy.*** Regulators expect institutions to maintain adequate capability in this area, but a specific cyber-strategy is typically not required.
- ***Cyber-risk management.*** For most jurisdictions, "broader IT and operational risk management practices are quite mature and are used to address cyber-risk and supervise cyber-resilience." Furthermore, "jurisdictions expect banks to have a strategy and framework to comprehensively map and actively manage their IT system architecture."
- ***Governance/organization.*** "[C]yber-resilience is not always clearly articulated across technical, business and strategic lines," contributing to a "confusion in roles and responsibilities," which ultimately "hampers the effectiveness" of the "three lines of defense" model.
- ***Workforce.*** A shortage of skilled workers in this field has contributed to recruitment challenges. In a few jurisdictions, cyber-certifications have been implemented or leveraged to address this.
- ***Testing.*** While protection and detection testing is prevalent and evolving, incident response and recovery testing is less prevalent. "Incident response and recovery testing is typically done through tabletop exercises, and broader continuity testing."
- ***Incident response.*** For all jurisdictions, supervisors "expect banks to prepare an incident response plan to deal with material cyber incidents." Additionally, banks are expected to classify information assets and services based on "operational sensitivity and business criticality."
- ***Assessment metrics.*** While some forward-looking indicators of cyber-resilience are "picked up through the most widespread supervisory practices, no standard set of metrics has emerged yet," making it more difficult for supervisors and banks to "engage on cyber-resilience."
- ***Information-sharing.*** The most commonly observed information-sharing practices involve communications among banks, mostly on a voluntary basis, and communications between banks and regulators.
- ***Third-party risk.*** With respect to outsourcing activities across jurisdictions, regulatory frameworks are well-established and share many similarities. These frameworks are being used by supervisors to indicate expectations with respect to banks' management of third-party dependencies. However, the Basel Committee found no common approach with respect to third parties aside from outsourced services. Notably, the responsibility falls on the financial institution to demonstrate adequate understanding and management of third-party risks.

2. Cyber-Resilience Standards and Guidelines

According to the report, most jurisdictions view cyber-resilience through the lens of IT and operational risk. Standards for general risks, including business continuity planning and outsourcing, contribute to the

management of cyber-risk, while specific guidance on cyber-risk management or information security guidance has emerged in a few jurisdictions (such as Hong Kong and Brazil). Where specific guidance does not exist, supervisors have encouraged financial institutions to look to international standards and prescriptive guidance. Supervisors in most jurisdictions leverage key concepts from international and industry standards such as NIST, ISO/IEC and COBIT, and supervisory practices from the U.S., such as the Federal Financial Institution Examining Council (FFIEC) IT Examination Handbook, and the UK, such as CBEST.

3. Governance Arrangements and Culture.

The Basel Committee found that regulatory and supervisory practices generally address enterprise IT risk management, but do not specifically address critical business functions, interconnectedness or third-party risk management. Against this context, the Basel Committee identified supervisory expectations and practices in five areas relevant to cyber-governance: (1) cybersecurity strategy; (2) management roles and responsibilities; (3) cyber-risk awareness culture; (4) architecture and standards; and (5) cybersecurity workforce.

The Basel Committee found that while most regulators do not require development of a cybersecurity strategy, "all expect regulated institutions to have a board-approved information security strategy, policy and procedures."

The report also described a general recognition of the importance of the board of directors and senior management in cyber-governance, highlighting how "[s]ome jurisdictions have issued specific regulatory guidance and requirements" concerning the responsibilities of the board of directors and senior management in this area. Many jurisdictions stress the importance of management's responsibilities with respect to cyber-governance and controls.

The Basel Committee noted that employees' awareness of cyber-risk and a common risk culture across the banking industry are foundational to maintaining cyber-resilience. Published guidance has been distributed by regulators in most jurisdictions that emphasizes the importance of risk awareness and culture for employees at all levels. Some regulatory requirements include increasing cybersecurity awareness and staffing, and, in some jurisdictions, regulators require cybersecurity awareness training throughout the term of employment. With respect to "insider threats" and third-party vendor risk, some jurisdictions may require background verification and screening for new employees and non-disclosure clauses in employee agreements, and may assess whether banks have processes and procedures to ensure that employees, contractors and third-party vendors "understand their responsibilities, are suitable for their roles and have the requisite skills to reduce the risk of theft, fraud or misuse of facilities." Regulators may also review a "bank's cyber-risk appetite, considering such factors as the bank's business model, core business strategy and key technologies."

According to the report, the architecture and standards of an institution's cybersecurity framework are not specifically mandated by most regulators, with only a few regulators giving specific guidance or consideration to this topic. U.S. regulators are among the exceptions that do provide specific guidance.

With respect to the cybersecurity workforce, the report found that "the skills and competencies of [the workforce], their regulatory frameworks and the range of practices differ markedly across jurisdictions." Most jurisdictions "are in the early stages of implementing supervisory practices to monitor a bank's cyber-workforce skills and resources," noting that the majority "assess the cybersecurity workforce of the institutions through on-site inspections."

4. Approaches to Cyber-Risk Management.

The Basel Committee describes a range of observed practices on cyber-risk management, and incident and response and recovery, which it discusses in four areas: (1) methods for supervising cyber-resilience; (2) information security controls and testing; (3) response and recovery testing; and (4) cybersecurity and resilience metrics.

In terms of supervision, most jurisdictions focus on cyber-risk "in the context of the [institution's] scale, complexity, business model and previous findings." Half of EU jurisdictions have internal guidance addressing when cybersecurity review should be conducted. "Most jurisdictions [perform] off- and on-site reviews and inspections of regulated institutions' information security controls to assess compliance with regulatory standards and alignment with good practice." In addition, jurisdictions are increasingly engaging with industry either to influence industry behavior, or to seek feedback and views to information regulators' work in this area.

With respect to information security controls testing and independent assurance, the report notes that most jurisdictions view mapping and classifying the institution's services and supporting assets and services as important in establishing cyber-resilience. In addition, supervisors review and challenge banks' approach to testing controls and remediation of identified issues through reviews of documents such as surveys or risk assessments. The report also notes that regulators review and challenge companies' approach to testing controls. However, some jurisdictions take a more active approach, including five EU jurisdictions that perform regulator-led penetration testing.

In terms of response and recovery testing, regulators evaluate whether an institution's service continuity plans align with other risk managing frameworks or strategies in the organization (for example, business continuity or risk frameworks, IT disaster recovery plans and data center strategies). A majority of regulators require these types of frameworks or policies, which address prevention, detection, response, recovery and reporting. Specific requirements vary, and most are not specific to cyber-risk. Among others, the report noted that supervisory guidance in the U.S. addresses "incident management, covering identification of indicator of compromise, analysis and classification of events, and escalation and

reporting of incidents." The Basel Committee also noted that several jurisdictions, including the U.S., complete a post-incident review of the institution's response and the root cause analysis.

In addition to testing, the report also noted that most supervisors and banks use exercises to prepare for incident response.

With respect to metrics, the report identifies the use of cybersecurity and resilience metrics as an important, but still immature, method for regulatory assessments and benchmarking. The report notes that, although some jurisdictions have created indicators based on their review of cyber-related information, none has developed quantitative metrics.

5. Communications and Information-Sharing.

The report also focuses on the various types of cybersecurity information-sharing mechanisms established by Basel Committee jurisdictions, including: (1) banks sharing information with each other; (2) banks sharing information with regulators; (3) regulators sharing information with each other; (4) regulators sharing information with banks; and (5) banks and regulators sharing information with security agencies. The report notes that the type of information shared varies depending on the practice, but may include information relating to threats, incidents, regulatory and supervisory responses, and best practices.

The Basel Committee notes that jurisdictions with observable practices for information-sharing among banks tend to have less robust practices with respect to information-sharing by regulators with banks. This was attributed to a reduced need for information-sharing by regulators if the peer sharing practice among banks is operating effectively. Relatedly, where jurisdictions exhibited greater information-sharing by banks with regulators, there were lower rates of information-sharing with security agencies.

With respect to information-sharing among banks, the report notes that there is no common standard, but that many jurisdictions have established voluntary sharing practices for vulnerabilities, threats, incident information and even indicators of compromise in some cases. These practices may be established via public or private sector platforms, depending on the jurisdiction, with some establishing joint public/private forums or government-led centers.

Information-sharing by banks with regulators is typically focused on sharing of cyber-incidents based on mandatory reporting requirements. The range of regulatory reporting requirements varies among jurisdictions and may depend on the type of authority, the mandate, the sector, and the geographic scope. Although many supervisors focus on reactive reporting, some have taken a more proactive approach with respect to tracking non-materialized threats.

With respect to sharing among regulators, the report notes that "[r]egulators share information with fellow regulators, be they domestic or cross-border, as appropriate according to established mandatory or voluntary information-sharing arrangements." At the same time, considering the many types of

cybersecurity information-sharing, the report observes that information-sharing among regulators is the "least observed practice across jurisdictions" when compared with the other types of information-sharing described above. The Basel Committee notes the importance of information-sharing among regulators as cyber-fraud becomes increasingly sophisticated and global.

Various jurisdictions have established standards and practices for information-sharing by regulators with banks. Generally, the regulator receives the information, assesses the risk to the industry, and determines whether the information should be passed along. Depending on the sensitivity of the information, it may be anonymized or shared via informal meetings or communications. Only a few jurisdictions (for example, China) impose mandatory requirements for regulators to share information and a few others have put in place voluntary practices (for example, Singapore and the UK), meaning many jurisdictions do not have set practices in this area.

Finally, the report stresses the importance of communications between banks and security agencies to "facilitate broader awareness" of threats, which may extend beyond the financial industry. Most jurisdictions adopt a voluntary approach with respect to information-sharing with security agencies, with a few jurisdictions imposing formal information-sharing requirements.

6. Interconnections with Third-Party Service Providers.

The Basel Committee's report next focuses on the increased challenges associated with extensive use of third-party services, including: (1) outsourcing, such as cloud computing services; (2) non-outsourced services and products, such as software or telecommunication lines; and (3) interconnected counterparties, such as other institutions and financial market infrastructures (for example, payment and settlement systems). Specifically, the report addresses the governance of third-party interconnections; business continuity and availability; information confidentiality and integrity; specific expectations and practices concerning visibility of third-party interconnections; auditing and testing; and resources and skills.

In terms of governance, regulations largely require the development of a management- and/or board-approved outsourcing framework. Regulators often require institutions to implement a comprehensive contractual framework setting forth the specifications of the service, the expected results of outsourcing, and the respective roles and responsibilities of the parties. In addition, risk assessments and contracts are typically expected to include analysis and clauses on a variety of risks, including, but not limited to, strategic, compliance, and business continuity risks. Furthermore, regulators often expect frameworks to be designed "to ensure the availability of critical systems and the security of sensitive data." The Basel Committee noted widespread practices of on-site inspections, and off-site review of statements and reports addressing outsourcing policies and risks of the financial institutions.

Regarding business continuity and availability, the report finds that regulators typically request that financial institutions design and implement appropriate plans, procedures, and technical solutions to

address the "availability and continuity of critical business activities" in the event of exceptional crises, such as cyber-incidents. In the same vein, regulators have also stressed the importance of aligning business continuity plans with those of critical service providers or suppliers. Most regulators expect financial institutions to test these measures periodically to measure efficacy.

The report notes that general data protection requirements commonly address "[c]onfidentiality and integrity of information for third-party interactions." Banks are commonly required to take steps to ensure third-party providers protect the confidential information of the institution and its clients. Increasingly, jurisdictions are imposing specific requirements for cloud computing services, including requirements related to data location and segregation.

Supervisory authorities in many jurisdictions request notification of material outsourcing agreements and may impose conditions on them, such as "preserving a minimum level of visibility" for outsourced functions. Institutions may be expected to keep an inventory of their outsourced functions and receive regular reports from service providers. Ultimately, the report found great variation in terms of the scope, format and content of information requests in this area.

For auditing, the majority of requirements emphasize the necessity of guaranteed "rights to inspect and audit" service providers. For several jurisdictions, the view on auditing outsourcing arrangements may be formed based on the service provider's external auditor, whereas other jurisdictions accepted pooled audits from multiple financial institutions or the internal audits of a service provider, subject to compliance with regulatory conditions. Institutions are typically required to monitor service providers' compliance with security requirements.

Finally, the report addresses resources and skills, indicating that banks may require specialist insight as to whether effective oversight is maintained over emerging technologies. The expectation is generally that relevant personnel have the requisite expertise to monitor outsourced services and manage any associated risks. In addition, there is an expectation that institutions will provide for sufficient personnel to ensure "continuity in managing and monitoring" in this area. Consultants or specialists may be necessary to supplement in-house personnel.

OBSERVATIONS

The Basel Committee's report is a sweeping survey of practices among banks, regulators and supervisors across jurisdictions with respect to cybersecurity resilience.[2] It creates no new requirements or immediate implications for financial institutions, but provides insight into practices in the industry and the increasing regulatory and supervisory focus on strengthening cyber-resilience both within institutions and across the sector.

* * *

ENDNOTES

[1] *Cyber-resilience: Range of practices*, Basel Committee on Banking Supervision (Dec. 4, 2018), http://www.bis.org/bcbs/publ/d454.pdf.

[2] In many cases, the general practices, requirements or behaviors described are different in the U.S.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York

Thomas C. Baxter Jr.	+1-212-558-4324	baxtert@sullcrom.com
Whitney A. Chatterjee	+1-212-558-4883	chatterjeew@sullcrom.com
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Elizabeth T. Davy	+1-212-558-7257	davye@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
Michael T. Escue	+1-212-558-3721	escuem@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Jared M. Fishman	+1-212-558-1689	fishmanj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
C. Andrew Gerlach	+1-212-558-4789	gerlacha@sullcrom.com
Wendy M. Goldberg	+1-212-558-7915	goldbergw@sullcrom.com
Charles C. Gray	+1-212-558-4410	grayc@sullcrom.com
Joseph A. Hearn	+1-212-558-4457	hearnj@sullcrom.com
Shari D. Leventhal	+1-212-558-4354	leventhals@sullcrom.com
Mark J. Menting	+1-212-558-4859	mentingm@sullcrom.com
Nader A. Mousavi	+1-212-558-1624	mousavin@sullcrom.com
Camille L. Orme	+1-212-558-3373	ormec@sullcrom.com
Stephen M. Salley	+1-212-558-4998	salleys@sullcrom.com
Rebecca J. Simmons	+1-212-558-3175	simmonsr@sullcrom.com
William D. Torchiana	+1-212-558-4056	torchianaw@sullcrom.com
Donald J. Toumey	+1-212-558-4077	toumeyd@sullcrom.com
Marc Trevino	+1-212-558-4239	trevinom@sullcrom.com

Benjamin H. Weiner	+1-212-558-7861	weinerb@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
William F. Kroener III	+1-202-956-7095	kroenerw@sullcrom.com
Stephen H. Meyer	+1-202-956-7605	meyerst@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Andrea R. Tokheim	+1-202-956-7015	tokheima@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com
Los Angeles		
Patrick S. Brown	+1-310-712-6603	brownp@sullcrom.com
William F. Kroener III	+1-310-712-6696	kroenerw@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com
Paris		
William D. Torchiana	+33-1-7304-5890	torchianaw@sullcrom.com
Melbourne		
Robert Chu	+61-3-9635-1506	chur@sullcrom.com
Tokyo		
Keiji Hatano	+81-3-3213-6171	hatanok@sullcrom.com
Hong Kong		
Michael G. DeSombre	+852-2826-8696	desombrem@sullcrom.com