MAYER | BROWN

May 4, 2020

Legal Update

Financial Stability Board Proposes Cyber Incident Response and Recovery Best Practices

On April 20, 2020, the Financial Stability Board ("FSB") released a "consultative document" on *Effective Practices for Cyber Incident Response and Recovery* (the "Proposal").[1] The Proposal requests public comment on a "toolkit" of effective practices designed to assist financial institutions in cyber incident response and recovery activities.[2]

The Proposal outlines practices for effective cyber incident response and recovery that are organized into seven broad categories that contain 46 practices. These practices will be familiar to many in the field and generally do not break new ground on best practices for response and recovery activities.

The Proposal is intended to provide a "toolkit" for institutions as well as a resource for national regulatory authorities in designing appropriate regulatory or supervisory programs. However, FSB does not intend for the Proposal to become a standard and explicitly states that it is "not a prescriptive recommendation for any particular approach."[3]

While the Proposal will not create new regulatory obligations for financial institutions, it may, if finalized, represent an important step forward in developing a common understanding of best practices that can be used by financial institutions and national regulators alike to evaluate current practices, set supervisory expectations, and engage in collaborative efforts to define and mitigate cybersecurity risk.

This Legal Update discusses the content and context of the Proposal and identifies how it would fit within the respective cybersecurity frameworks as well as key takeaways for financial institutions in the United States and in the Europe Union ("EU").

Background

The FSB was established in 2009 by the governments of the Group of Twenty ("G20") to provide international coordination among national financial regulatory authorities, international financial institutions, and international standards bodies to develop international standards and make policy recommendations to address vulnerabilities and promote financial system stability.[4] Policy recommendations and decisions of the FSB are not legally binding on any of its members; however, policy recommendations are designed to establish international standards to promote financial stability that are encouraged to be adopted by the national regulators in each member jurisdiction.[5]

Accordingly, FSB policy recommendations may be adopted by home country regulators as supervisory guidance or other regulatory mandate.

Cybersecurity issues have been a focus of the FSB's work in recent years. In 2017, the FSB surveyed the cybersecurity regulatory and supervisory practices of FSB member jurisdictions.[6] Noting a number of common features of national regulators' approaches, the 2017 survey identified a need for a "globally consistent approach" to regulation. To advance this goal, the FSB released a *Cyber Lexicon* in 2018 to provide a cross-sector common understanding of cybersecurity and cyber resilience terminology to support the work of the FSB, standards bodies, national regulators, and financial institutions.[7] As part of its 2019 work program, the FSB undertook a new initiative to develop effective practices relating to a financial institution's response and recovery from a cybersecurity incident.[8] The Proposal is the culmination of the FSB's efforts to capture effective practices for cyber incident response and recovery and is expected to be finalized in late 2020.[9]

Cyber Incident Proposal

The 46 practices discussed in the Proposal (reproduced in the Appendix to this Legal Update) are drawn from the 2017 survey of national regulators' guidance and approaches, a review of case studies on past cybersecurity incidents, an online survey of industry practices, and other engagements with FSB stakeholders. They are grouped into seven broad components: governance, preparation, analysis, mitigation, restoration, improvement, and coordination and communication. In addition to identifying and describing effective practices, the Proposal provides relevant definitions and examples (e.g., types of metrics used by industry to measure incident impact and performance of incident response programs). The Proposal does not address customer notification or related points typically covered in a jurisdiction's consumer breach notification law.

A. GOVERNANCE

The Governance component includes practices related to the framework for an institution's management of cyber incident response and recovery, such as defining the organizational structures, roles, responsibilities, and metrics to coordinate response and recovery across every facet of the institution's business. Effective practices in the Governance component include the development and adoption of an organization-wide governance framework; engagement by the board; clear roles, responsibilities, and accountability of senior management; and provision of adequate financial and human capital to a well-functioning cyber incident response and recovery capability.

B. PREPARATION

The Preparation component includes practices related to establishing and maintaining cyber incident response and recovery capabilities. The Preparation component consists of practices implemented before an incident that "significantly and directly" influence the effectiveness of the cyber incident response and recovery activities. Effective practices in the Preparation component include written policies that describe the organization's response and recovery processes; plans and playbooks to provide well-defined approaches to response and recovery activities; communications strategies and plans for engaging internal and external stakeholders; stress testing and scenario analysis to understand the full scope of possible incidents; and the establishment and maintenance of disaster recovery, forensic, and other technical and operational capabilities.

C. ANALYSIS

The Analysis component includes practices related to determining the severity, impact, and root cause of cyber incidents to drive appropriate response and recovery activities. Effective practices in the Analysis component include using a pre-established taxonomy for classifying cybersecurity incidents and a pre-established framework for assessing incident severity; identifying and collecting appropriate logs for timely analysis and investigation; collecting, verifying, and continuously monitoring information from computing resources across the organization; and accumulating threat intelligence information from trusted third-party sources.

D. MITIGATION

The Mitigation component includes practices designed to prevent aggravation of a cybersecurity incident and to assist in quickly eradicating the threat and minimizing the impact on business operations. Effective practices in the Mitigation component include activating threat-specific containment processes and technologies; invoking business continuity plans and contingency measures to (potentially manually) process critical transactions; shutting down or isolating affected systems and operations; and eradicating malicious artifacts and closing vulnerabilities to prevent reintroduction.

E. RESTORATION

The Restoration component includes practices designed to repair or restore impacted systems such that services can return to normal operation. Effective practices in the Restoration component include prioritizing restoration activities based on business needs and security and technical requirements; defining acceptable interim measures such as continuing operations with a diminished capacity while restoration is in progress; monitoring systems to identify abnormal activities and compromised assets; validating system recovery; and managing the restoration and ensuring the integrity of data.

F. IMPROVEMENT

The Improvement component includes practices designed to enhance readiness through exercises and tests that proactively build capabilities and post-incident analysis and reflection to assess adherence to and effectiveness of organizational policies and procedures. Effective practices in the Improvement component include tabletop exercises and live simulations; cross-sectoral and cross-border exercises, potentially with the participation of national regulatory authorities; integration of third-party technological tools and data sources; and post-incident analysis and assessment of lessons learned with internal and external stakeholders.

G. COORDINATION AND COMMUNICATION

The Coordination and Communication component includes practices designed to ensure effective, timely, and trusted communication with internal and external stakeholders to share progress, outcomes, and analysis throughout the lifecycle of the cybersecurity incident. Effective practices in the Coordination and Communication component include timely escalation of cybersecurity incidents within the organization; pre-defined communication intervals and formats to share actionable, timely, and concrete information regarding the incident and recovery processes; cross-border coordination developed, where possible, through engagement with national regulatory authorities; and trusted communications channels and processes.

Best Practices, What For?

The Proposal does not—nor is it intended to—provide a set of prescriptive recommendations or a fully functioning response plan for financial institutions to adopt or national regulatory authorities to enact. Furthermore, it is not intended to replace or supplement the state data breach notification laws or identify new best practices. Instead, the Proposal is designed to provide a toolkit that, much like the *Cyber Lexicon* released by the FSB in 2018, will offer a common understanding and taxonomy for effective practices in the cyber incident response and recovery arena that may be used to enhance response plans and cybersecurity requirements.

Key Takeaways for US Financial Institutions

FSB's approach in the Proposal aligns well with the recent posture of US financial regulators toward cybersecurity risk management and regulation. US financial regulators have been hesitant to impose prescriptive regulations on financial institutions for cybersecurity incident response and recovery activities, opting instead to focus on collaborative efforts with industry participants to reach a common understanding of cybersecurity risks.

In 2016, the Board of Governors of the Federal Reserve System ("Federal Reserve"), the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation issued a joint advance notice of proposed rulemaking ("ANPR") regarding enhanced cyber risk management standards applicable to large and interconnected financial institutions.[10] Although the comment period for the ANPR ended in early 2017, the supervisory agencies have not taken further action, and informal comments from agency staff have indicated that it is unlikely the ANPR will be finalized as a regulation.

More recently, US financial regulators have pivoted to focus on industry collaboration and harmonization instead of prescriptive regulation. For example, in a 2018 speech discussing cybersecurity supervision, Vice Chairman for Supervision of the Federal Reserve Randal Quarles (who currently is the Chair of FSB) noted that the Federal Reserve is focusing on "aligning our expectations with existing best practices" and introducing and participating in programs in partnership with the public and private sectors.[11]

In keeping with these priorities, the Federal Reserve has engaged industry participants in attempts to define and classify cybersecurity risks in financial risk management. One recent example of these efforts is a November 2019 cyber risk workshop organized by the Federal Reserve Banks of Richmond and New York to discuss proposed classification schemes and data collection schedules and structures.[12] Outside of the banking agencies, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") recently released a series of observations of effective practices—similar to the Proposal—collected from OCIE's examination of securities market participants regarding cybersecurity and operational resilience.[13]

While the release of the Proposal is unlikely to have significant near-term impacts on any cyber risk management expectations that may be imposed on US financial institutions, institutions should take note of the effective practices curated by FSB as regulators begin to coalesce around a common understanding of both cybersecurity risk and effective strategies to respond and recover from cyber incidents. In this regard, the Proposal may provide a useful toolkit to evaluate the current practices of a financial institution and could be incorporated into supervisory expectations going forward as supervisory agencies align their expectations with industry best practices.

Key Takeaways for European Financial Institutions

The EU cybersecurity landscape for financial institutions has not waited for FSB's work to evolve over the recent years. Both sector specific and overarching prescriptive cybersecurity rules have been adopted at the EU level and implemented among the various EU member states. To that end, the EU approach is very different from the US one.

The NIS Directive[14] was adopted on July 6, 2016, with an implementation deadline for member states on May 9, 2018. The NIS Directive introduced supervision and specific cybersecurity requirements on so-called operators of essential services ("OES"); the banking sector is one identified as in scope of the NIS Directive. Member states had to designate, among the institutions active within their territory, those that are considered OES. Strict cybersecurity preparedness and requirements apply to OES (and are pushed down the supply chain through contractual arrangements), and incident management and notification requirements are an important component. Various sets of guidelines published by the European Agency for Cybersecurity ("ENISA") and other EU bodies include guidelines on cyber incident preparedness and responses.[15]

The PSD2 Directive[16] includes a set of security measures that have to be met by payment services providers; developing incident management procedures is one important component identified. The PSD2 Directive, even if sector specific, applies broadly compared to the NIS Directive, as the PSD2 Directive does not include the requirement to be identified as "essential" by national authorities to be within its scope. In addition to domestic implementation, Europe-wide guidelines on major incident reporting were published by the European Banking Authority.[17]

Further, and with the broadest possible reach, the GDPR includes data breach notification regimes, as well as security requirements spread across the regulation. Organizations are accountable in the way they prepare for and deal with incidents compromising personal data. Properly dealing with them requires organizations to develop cyber incident response.

Having comprehensive frameworks in place applying to selection of key actors, sector-wise or more broadly across the spectrum of financial institutions, does not make the Proposal less relevant in the EU context. The Proposal might resonate differently, however. Indeed, the best practices might serve as a useful reference point to benchmark internal policies and rules against a broader accountability tool that not only deals with hard requirements but seeks to promote a culture of awareness and preparedness across an entire organization. Further, the Proposal might be used by national authorities when contemplating building a culture of trust across the sector they supervise and enforce.

Concluding Thoughts

There remains significant variability in financial institutions' understanding of and responses to cybersecurity risk, and these definitional variations pose significant challenges for financial institutions and national regulators alike in terms of quantifying, classifying, and evaluating cybersecurity risk. Efforts to harmonize this understanding are ongoing.

The release of the Proposal provides another data point that financial institutions and national regulatory authorities can use to help define best practices and evaluate organizational practices and priorities in light of industry trends. Like the *Cyber Lexicon* released by the FSB in 2018, the Proposal will promote a common understanding of practices, processes, and tools that can be used to harmonize financial industry participants' efforts in this arena.

Have your say and contribute to the Proposal by providing comments before July 20, 2020. Responses to this the consultation report should be sent to CIRR@fsb.org. An optional template for submitting responses to optional guiding questions can be downloaded.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

AUTHORS:

Rajesh De
+1 202 263 3366
rde@mayerbrown.com

Diletta De Cicco
+32 2 551 5945
ddecicco@mayerbrown.com

Charles-Albert Helleputte
+32 2 551 5982
chelleputte@mayerbrown.com

David A. Simon
+1 202 263 3388
dsimon@mayerbrown.com

Jeffrey P. Taft
+1 202 263 3293
jtaft@mayerbrown.com

Kelly F. Truesdale
+1 202 263 3294
ktruesdale@mayerbrown.com

Matthew Bisanz
+1 202 263 3434
mbisanz@mayerbrown.com

OTHER CONTACTS:

Gabriela Kennedy
+852 2843 2380
gabriela.kennedy@mayerbrown.com

Nicolette Kost De Sèvres
+1 202 263 3000
nkostdesevres@mayerbrown.com

Mark A. Prinsley
+44 20 3130 3900
mprinsley@mayerbrown.com

Oliver Yaros
+44 20 3130 3698
oyaros@mayerbrown.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

Endnotes

[1] FSB, *Effective Practices for Cyber Incident Response and Recovery* (Apr. 20, 2020), https://www.fsb.org/wp-content/uploads/P200420-1.pdf [*hereinafter* the "Proposal"].

[2] The FSB defines a "cyber incident" as a cyber event that (i) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. *See* FSB, *Cyber Lexicon* (November 2018).

[3] *Supra* note 1, at 2.

[4] History of the FSB (2020), https://www.fsb.org/history-of-the-fsb/.

[5] About the FSB (Nov. 8, 2014), https://www.fsb.org/about/.

[6] Press Release, *FSB publishes stocktake on cybersecurity regulatory and supervisory practices* (Oct. 13, 2017), https://www.fsb.org/2017/10/fsb-publishes-stocktake-on-cybersecurity-regulatory-and-supervisory-practices/.

[7] FSB, *Cyber Lexicon* (Nov. 12, 2018), https://www.fsb.org/wp-content/uploads/P121118-1.pdf.

[8] Press Release, *FSB reviews financial vulnerabilities and deliverables for G20 Summit* (Oct. 22, 2018), https://www.fsb.org/2018/10/fsb-reviews-financial-vulnerabilities-and-deliverables-for-g20-summit/.

[9] Press Release, *FSB updates G20 on its work related to cyber incident response and recovery* (May 28, 2019), https://www.fsb.org/2019/05/fsb-updates-g20-on-its-work-related-to-cyber-incident-response-and-recovery/.

[10] Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74315 (Oct. 26, 2016).

[11] Speech to Financial Services Roundtable 2018 Spring Conference, Randal K. Quarles, *Brief Thoughts on the Financial Regulatory System and Cybersecurity* (Feb. 26, 2018) https://www.federalreserve.gov/newsevents/speech/quarles20180226b.htm.

[12] Cyber Risk Workshop, Federal Reserve Bank of Richmond (Nov. 20, 2019), https://www.richmondfed.org/conferences_and_events/banking/2019/20191120_cyber_risk_workshop.

[13] *See* Mayer Brown, *Legal Update: SEC's OCIE Publishes Observations on Cybersecurity and Resiliency Practices* (Feb. 25, 2020), https://www.mayerbrown.com/en/perspectives-events/publications/2020/02/secs-ocie-publishes-observations-on-cybersecurity-and-resiliency-practices.

[14] EU 2016/1148 Directive on security of network and information systems.

[15] See, ENISA, Mapping of OES Security Requirements to Specific Sectors (Dec. 2017), https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/; NIS cooperation group, Reference document on security measures for Operators of Essential Services (Feb. 2018), https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf.

[16] EU 2015/2366 Directive on payment services in the internal market.

[17] Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2) (July 27, 2017), https://eba.europa.eu/sites/default/documents/files/documents/10180/1914076/3902c3db-c86d-40b7-b875-dd50eec87657/Guidelines%20on%20incident%20reporting%20under%20PSD2%20(EBA-GL-2017-10).pdf.

Appendix: Listing of Effective Practices by Component

GOVERNANCE	PREPARATION
Organization-wide governance framework Role and responsibilities of the board Roles, responsibilities, and accountabilities for cyber incident response and recovery Executive sponsorship Culture Funding Human resources Metrics	Policies Plans and playbooks Communication strategies, channels, and plans Scenario planning and stress testing Security Operations Center (SOC) Disaster recovery sites Forensic capabilities Technology solutions and vendors Supply chain management Third-party cyber services providers
ANALYSIS	**MITIGATION**
Cyber incident taxonomy System and transaction logs Trusted information sources	Containment Business continuity measures Isolation Eradication
RESTORATION	**IMPROVEMENT**
Prioritization Key milestones Monitoring Approved restoration procedures Validation Record activities Data recovery “Golden source” data	Exercises, tests, and drills Cross-sectoral and cross-border exercises Technological aids External events and sources Industry-wide initiatives Post-incident analysis Lessons learned
COORDINATION AND COMMUNICATION	
Timely escalation Regular updates with actionable messages Cross-border coordination Trusted information sharing Trusted communication channels Cyber incident reporting	

Mayer Brown is a distinctively global law firm, uniquely positioned to advise the world's leading companies and financial institutions on their most complex deals and disputes. With extensive reach across four continents, we are the only integrated law firm in the world with approximately 200 lawyers in each of the world's three largest financial centers—New York, London and Hong Kong—the backbone of the global economy. We have deep experience in high-stakes litigation and complex transactions across industry sectors, including our signature strength, the global financial services industry. Our diverse teams of lawyers are recognized by our clients as strategic partners with deep commercial instincts and a commitment to creatively anticipating their needs and delivering excellence in everything we do. Our "one-firm" culture—seamless and integrated across all practices and regions—ensures that our clients receive the best of our knowledge and experience.

Please visit mayerbrown.com for comprehensive contact information for all Mayer Brown offices.