Basel Committee Publishes Report on Cyber-Resilience Practices

December 14, 2018

On December 4, 2018, the Basel Committee on Banking Supervision published a report on "Cyber-resilience." The report identifies, describes and compares the range of observed bank, regulatory and supervisory cyber-resilience practices and expectations across jurisdictions and is intended to help banks and supervisors "navigate the regulatory environment."[1] In surveying the general cyber-resilience landscape, the Basel Committee finds that:

Debevoise & Plimpton

- Most regulators leverage previously developed national or international standards for cyber-resilience—principally the NIST, ISO and CPMI-IOSCO frameworks;
- Although regulators generally do not require a specific cyber strategy, all expect institutions to maintain adequate capability in this area; and
- In most jurisdictions, cyber-risk and cyber-resilience are addressed through broader and well-established IT and operational risk management practices.

The report discusses practices and expectations across four broad dimensions of cyber-resilience: (1) governance and culture, (2) risk measurement and assessment of preparedness (both in prevention and recovery/learning), (3) communication and information sharing and (4) interconnections with third parties. Below, we briefly discuss these areas of focus and note the Basel Committee's key findings.

GOVERNANCE AND CULTURE

- *Governance/organization*. Although management models, such as the three lines of defense model, are widely adopted, cyber-resilience is not always clearly articulated across technical, business and strategic lines.
- *Workforce*. Skills shortages in the field of cyber-security lead to recruitment challenges.

[1] The findings in the report are based on survey data from the Basel Committee's member jurisdictions taken in April 2017.

The Basel Committee's concern that, within management models, cyber-resilience is not always "clearly articulated" appears consistent with regulatory focus in the United States. For example, Securities and Exchange Commission guidance from February of this year stresses the importance of developing comprehensive controls and procedures around cyber-security.[2] A clear articulation of responsibilities, and how different lines should interact, is a necessary part of any such comprehensive controls and procedures.

RISK MEASUREMENT AND ASSESSMENT OF PREPAREDNESS

- *Testing*. While protection and detection testing are evolving and prevalent, incident response and recovery testing are less so.

- *Incident response*. Supervisors across all jurisdictions expect banks to have prepared an incident response plan for when material cyber incidents occur.

- *Assessment metrics*. A standard set of cyber-resilience metrics has yet to emerge, making it difficult for supervisors and banks to communicate clearly and consistently on these issues.

Because the report is intended to highlight potential areas for further policy work by the Basel Committee, it is possible that we may see an attempt to develop a standard set of cyber-resilience metrics.

COMMUNICATION AND INFORMATION SHARING

- *Information sharing*. Most information sharing regarding cyber incidents takes place among banks (typically on a voluntary basis) and between banks and regulators. Regulator-to-regulator communications, both domestically and cross-border, are less documented or systematic. Few jurisdictions have taken specific formal steps to facilitate the "speed, latitude, security and fluidity of communications" necessary to address cross-border cyber-incidents.

The report notes that public disclosure about cyber-security incidents and risks is another important form of information sharing. Public disclosure of cyber-related incidents has been a key focus for U.S. regulators and is discussed in the SEC guidance mentioned above.

---

[2] We discuss the SEC's guidance in further detail here.

INTERCONNECTIONS WITH THIRD PARTIES

- *Third-party risk.* Across jurisdictions, regulatory frameworks for outsourcing activities are well-established and share commonalities. However, there is no common approach regarding third parties beyond outsourced activities. The burden remains on banks to demonstrate adequate understanding and management of third-party risks.

In the United States, regulators appear keenly aware of the overall breadth and scope of third-party risks. For example, the SEC recently released an investigative report identifying instances of cyber-fraud using vendor credentials and stressed the importance of focusing on these types of third-party risks, noting that certain cyber-fraud strategies involving vendors may present fewer red flags.[3]

Some international standards, meanwhile, recognize that institutions may critically depend on third parties in ways other than those that are normally considered outsourcing activities. The ISO standards, for example, include requirements for managing risks associated with hardware, software, telecoms, applications, third-party hosting services, utilities and even environmental issues.

[3] We discuss the SEC's report in further detail here.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Matthew E. Kaplan
mekaplan@debevoise.com

Jim Pastore
jjpastore@debevoise.com

David L. Portilla
dlportilla@debevoise.com

Paul M. Rodel
pmrodel@debevoise.com

Sandeep S. Dhaliwal
ssdhaliwal@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com