A closer look

April 2015

A publication of PwC's financial services regulatory practice

Cyber: Think risk, not IT

Overview

Despite millions of dollars spent on enhancements, cybersecurity remains the area of risk management with the largest gap between threat and preparedness. As the frequency and sophistication of cyber attacks have increased significantly in recent years, counter measures have failed to keep pace.

This gap is especially important for financial institutions, which by our estimate are over 30% more likely to be targeted by cyber crime. While the biggest banks have been dealing with cyber threats for years, they and their smaller peers are largely responding to threats reactively. More specifically, banks continue to address past issues rather than responding to real-time and future threats via on-going monitoring of emerging cyber threats.

Three major factors contribute to financial institutions' cyber vulnerability. First, financial institutions are highly desirable targets for cyber criminals due to the centralization of data that they hold, which can be easily monetized. Second, due to technological advances, more sophisticated tools are increasingly available to cyber criminals at a reduced cost, making their attacks easy to scale and customize. Third, cyber crime is increasingly becoming a weapon in cross-border commercial or political disputes where state-sponsored hackers (with access to virtually unlimited resources) target US financial institutions.

In response, there has been a significant increase in regulatory discourse and issuances regarding cybersecurity, but regulators are still figuring out exactly what to do. Their efforts are evolving and have been largely advisory rather than enforcement-oriented. We believe it is only a matter of time before federal banking regulators begin singling out specific large institutions for robust examinations, using Matters Requiring Attention (MRAs) where they determine that risk management processes are insufficient.

At this point in time, the best option for financial institutions is to become cyber resilient, especially given cyber crimes' financial and reputational impact. To do so, banks should enhance their risk management processes to better identify and monitor cyber threats. This framework must be adopted on an enterprise-wide basis, beyond the IT department, that includes oversight and meaningful engagement by senior management and by the board of directors. Furthermore, the organizational standing of cyber risk should be elevated to parallel the statuses of credit, market, and other major risk categories (i.e., cybersecurity cannot remain a subset of operational risk).

This **A closer look** provides (a) an overview of the current state of cyber risk management practices, (b) an analysis of the regulatory response to the recent uptick in cyber threats, and (c) our view on what financial institutions should be doing to become cyber resilient.

pwc

Current state of cyber risk management

While the financial services industry has been more responsive to cyber risk than other industries, financial institutions still have a great deal of work to do to become cyber resilient. Larger banks have for some time now viewed cyber risk as an issue that goes beyond just the IT department. However, many are yet to elevate the status of cyber risk to a major risk category (e.g., credit or market risk) or to actively involve their senior management and board in cyber risk management.

The problem is further exacerbated by the following common issues we observe:

- *Lack of enterprise-wide processes and governance*: Threat monitoring and analysis at most financial institutions remain spread across multiple locations, and are performed by a combination of internal and external resources that use different tools, methodologies, and platforms that often do not communicate with each other. Similarly, financial institutions often lack centralized governance of cyber risk (e.g., centered around the Chief Risk Officer (CRO) or Chief Operating Officer (COO), with board engagement) resulting in limited enterprise-wide awareness and coordination.
- *Insufficient security systems and controls*: While many financial institutions currently have processes in place to actively manage business risk, most lack sophisticated and flexible tools and processes to monitor, analyze, and mitigate cyber risk. Cybersecurity systems at most firms are one-size-fits-all solutions that are designed to meet minimum standards and lack the capability to evolve as the profile of cyber threats changes.
- *Reluctance to share intelligence*: Intelligence on a specific cyber threat often remains within the group that deals with the threat. Rarely are efforts made to reach out to other parts of the organization (e.g., other business lines) to assess whether similar threats have been detected by them and to coordinate the response. Similarly, timely sharing of intelligence within the industry, and with outside authorities (e.g., regulators and law enforcement) is not common practice, although it would help serve as an early warning system.

Regulatory response

Given its history of coordinating regulatory IT examinations, it is not surprising that the Federal Financial Institution Examination Council (FFIEC)[1] has taken the initiative. The FFIEC performed pilot reviews of community banks last summer and issued its results in November 2014. We believe the FFIEC reviews focused on these institutions as they often lack the experience and resources of their larger peers in responding to cyber threats, and are more heavily reliant on third-party service providers (which are one of the weakest links in banks' cyber protection).

The FFIEC's report based on these reviews did not explicitly require any changes in the institutions' cybersecurity practices. Rather, it encouraged banks to share cybersecurity information with their peers and with regulators to enhance risk assessment and monitoring across the industry. The FFIEC report also called for banks to (a) increase the board and senior managements' awareness of the firm's cybersecurity risks, (b) establish a dynamic control environment and monitor threats enterprise-wide, and (c) incorporate cyber risk in their continuity and disaster recovery plans.

Building on these reviews, the FFIEC updated its IT examination handbook to focus on third-party service providers in February 2015, in order to hold banks accountable for cyber resiliency when using outsourced technology services. Despite the update's limited scope (i.e., addressing cyber resiliency in the context of business continuity planning), it is important as it formally introduces the concept of cyber resilience and evidences that cybersecurity-focused exams are on their way.[2]

We do not expect the federal banking agencies to issue guidance on their own beyond the FFIEC's initiatives in the near term.[3] Rather, their cyber examinations will evolve (e.g., putting greater emphasis on cyber risk management and readiness), using the FFIEC

[1] The FFIEC is a regulatory council composed of the Federal Reserve Board, Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation, Consumer Financial Protection Bureau, and the National Credit Union Administration.

[2] Last month, the FFIEC announced additional initiatives to eventually offer banks a cybersecurity self-assessment tool and to facilitate information sharing between its member agencies (among other initiatives). The FFIEC has also been issuing periodic statements to notify banks of increased threats of certain cyber attacks (as examples, it issued two in late March regarding destructive malware and the compromising of credentials).

[3] However, the CFTC, which is not an FFIEC member, has recently indicated that it is considering issuing regulations for financial market utilities. See PwC's *A closer look*, *Financial market utilities: Is the system safer?* (February 2015).

examination handbook as a basis. For example, the New York Fed's Executive Vice-President, Sarah Dahlgren, last month said her agency has formed a new unit for establishing a new risk-based cybersecurity assessment framework.

Going forward, as the adverse consequences of systems breaches continue to increase, enforcement actions will become more likely – especially if bank data is compromised due to weaknesses within the bank or a third party vendor (as opposed to, e.g., a breach at a retailer).

Delineated below are some of the key actions other government bodies have taken recently:

Federal agencies

Federal efforts to address cybersecurity risk outside of the FFIEC have also so far been principles-based, giving financial institutions much discretion in managing their cyber risk. FINRA's February 2015 report on its examination of registered broker-dealers highlights industry best practices. Like the FFIEC, the report focuses on a sound governance framework and third-parties, finding inadequate vendor oversight and supervision of outsourcing arrangements as a common deficiency. The FINRA report also points out broker-dealers' failure to safeguard confidential customer information, including a lack of adequate data protection measures (e.g., access control and encryption), and encourages firms to obtain adequate cybersecurity insurance (a call echoed by other regulators as well in public statements).

Also in February 2015, the SEC issued an assessment of broker-dealers and investment advisors it examined. Its report highlights the urgency of the cybersecurity problem by pointing out that 88% of the broker-dealers and 74% of the investment advisors examined experienced cyber attacks directly or through their vendors. Furthermore, over half the broker-dealers reported receiving fraudulent emails seeking to transfer client funds. However, the report points out that part of the problem could be solved by employees simply following existing processes, noting that a quarter of the losses would have been avoided if employees followed identity authentication procedures.

State agencies

Similar to the FFIEC's recent actions, the new cybersecurity examination guidelines issued last December by the New York Department of Financial Services (DFS) also emphasizes making banks more cyber resilient through the examination processes. The issuance sets out cybersecurity-specific areas to be included in the DFS's IT examinations, with an emphasis on: governance, management of third-party service providers, periodic review of written cybersecurity policies and procedures, ongoing cybersecurity testing and monitoring, personnel training, and integration of cybersecurity into business continuity and disaster recovery procedures.

In a speech last month, DFS Superintendent Benjamin Lawsky reiterated that targeted cyber exams were coming, and the exams would emphasize third party vendor risks and user authentication systems. DFS then followed up with a report this month indicating that it is considering issuing cybersecurity regulations aimed at banks' relationships with third parties.

The White House

Finally, the President has issued two pertinent executive orders this year. On April 1st, his Administration established the first-ever economic sanctions program in response to cyber attacks. Although no individuals or entities have yet been designated for asset freezes, we believe the Administration has specific designees in mind.[4]

In February, the President issued an executive order calling for more effective information sharing within the industry, and between the industry and government, building on the National Institute of Standards and Technology (NIST) framework for communicating cybersecurity issues. Most importantly, the order aims to expand collaboration through the creation of Information Sharing and Analysis Organizations (ISAOs), which will be more open than today's forums and are expected to use automated mechanisms for information sharing.[5] However, the ISAO program is voluntary and the establishment of ISAO standards for automated information sharing will take some time.

Although information sharing is no doubt useful in mitigating cybersecurity risks, information sharing exercises have had difficulty achieving their objectives. The private sector has been reluctant to share proprietary and potentially incriminating information about cyber breaches that may result in shareholder or customer lawsuits, especially in the absence of adequate cybersecurity insurance or liability limitations.

---

[4] See PwC's *Regulatory brief, Sanctions: US action on cyber crime* (April 2015) for more information.

[5] See PwC's *Cybersecurity Blog, Why Obama's executive order on cybersecurity information is on the mark* (February 2015) for more information.

What should financial institutions be doing now?

Regardless of the timing and details of future government action on cybersecurity, financial institutions should be working today to become cyber resilient. Given the evolving nature of cyber threats, an organization's response must be ongoing and iterative. The cyber risk management framework should evolve as the organization gains more insight into the nature, scope, and location of threats.

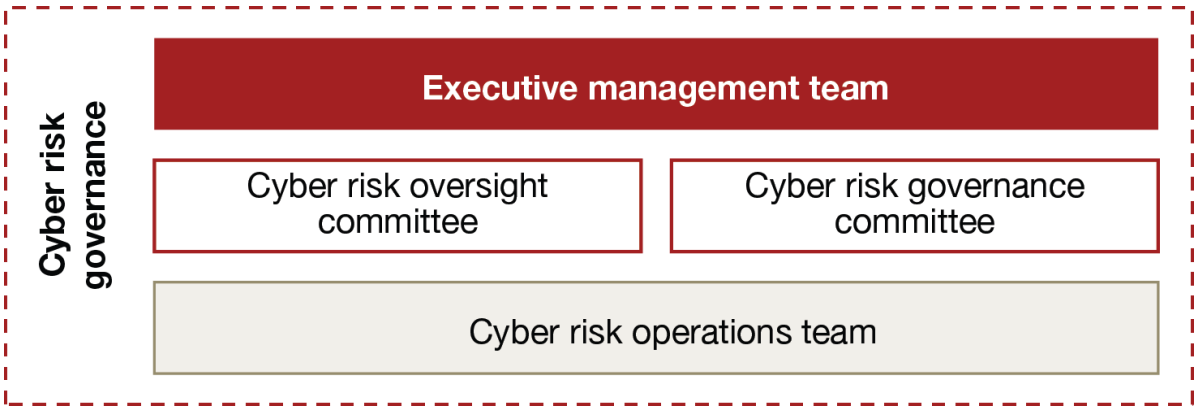
Accordingly, in our view financial institutions should take the following baseline steps:[6]

1. Establish a cyber risk governance framework that engages the board

The foundation of a cyber resilient organization is a cyber risk governance framework that is built into the larger enterprise-wide risk management framework, covering the organization's day-to-day activities. Cyber resilient organizations are those that have cyber risk expertise within their senior management ranks and their boards, and a detailed action plan to respond to cyber events (e.g., attacks, system breaches, etc.).

An effective risk governance framework should include a cyber risk governance committee, a cyber risk oversight committee, and a cyber risk operations team. Each of these should have clear responsibilities, operating processes, and reporting lines.

The following graphic displays the hierarchical relationship between the three committees and the executive management team.



Cyber risk governance committee

The cyber risk governance committee works directly with the firm's entire executive management team to develop the bank's cyber risk strategy, and informs and seeks input from the board.

Key members	Responsibilities
• Chief Operating Officer • Chief Risk Officer • Head of security • Heads of business lines and certain functional areas (such as business continuity planning, legal, risk, compliance, and regulatory)	• Collaborating with executive management to develop the bank's cyber risk strategy • Identifying critical information assets • Setting the budget for cyber risk management and ensuring appropriate investment in related cyber risk awareness training • Monitoring the firm's cyber risk position and reporting it to executive management and the board • Reviewing reports from the cyber risk oversight committee and cyber risk operations team to help prioritize emerging threats • Reassessing cyber risk strategy periodically to adapt to changes in the risk landscape

[6] See PwC's *Financial services viewpoint, Threat smart: Building a cyber resilient financial institution* (October 2014) for more information.

Cyber risk oversight committee

The cyber risk oversight committee is largely in charge of assessing existing and emerging cyber threats, and the effectiveness of the bank's response to these threats. In doing so, the committee directly oversees the firm's cyber risk operations team.

Key members	Responsibilities
• IT team • Business support teams • Business teams	• Assessing the active risks the organization faces • Evaluating the effectiveness of the cyber risk operations team • Identifying emerging threats and strengthening internal controls to improve protection of information assets • Determining how business changes affect the firm's cyber perimeter, e.g., new service offerings, suppliers, vendors, or business partners • Monitoring the status of updates and configuration changes to critical systems • Monitoring metrics that provide visibility on the performance of key elements of the firm's cybersecurity program • Overseeing employee training programs • Reviewing new regulatory and compliance requirements

Cyber risk operations team

The cyber risk operations team is the firm's first line of defense against cyber threats. The team is in charge of detecting and responding to cyber threats in real time, and reports to both the cyber risk governance and cyber risk oversight committees.

Key members	Responsibilities
• Managers with operational experience in networks, information security, fraud, and corporate security • Security operations center	• Serving as the first line of defense for detecting and responding to cyber events • Compiling real-time intelligence from all the groups that monitor cyber threats • Producing reports for the cyber risk oversight and governance committees on number and type of cyber events, origination and duration of events, targeted assets, attempted frauds, cyber risk mitigation enhancements, and comparison of events to industry trends

2. Adopt an enterprise-wide approach to cybersecurity that goes beyond the IT department

Define your cyber perimeter

An organization's cyber vulnerabilities extend to all locations where its data is stored, transmitted, and accessed – by third party service providers, employees, and customers. Pervasive use of cloud computing and mobile applications in recent years has expanded this perimeter beyond the institution's data centers and connected terminals (e.g., ATMs and wire transfer systems). Therefore, an accurately defined cyber perimeter should extend beyond the areas that the firm directly controls (e.g., its physical network) to cover third parties, outsourced data centers, customers, and the cloud. Once defined, the firm's cyber perimeter should be revisited and adjusted as needed considering changes in operations, business environment, and the industry.

Identify your critical business processes and assets across the organization

Putting equal priority on defending all assets within this perimeter is not practical, cost effective, or necessary. To optimize cyber efforts, financial institutions should identify their most valuable revenue streams, business processes, assets (including brand), and facilities, and determine where they are located and who has access to them. Cyber resilient financial institutions should also establish a risk tolerance level and assign executive responsibility for each of these valuable assets and processes. One result of these analyses may be establishing "multi-factor" authentication systems that go beyond the use of a username and password, as the FFIEC, FINRA, DFS and others have suggested.

Be prepared to respond

Each group within the cyber risk governance structure (i.e., the governance and risk oversight committees and the risk operations team) should develop prepared responses (i.e., playbooks) that specify who should take action, what their responsibilities are, and what they should do in case of a cyber event. Special attention must be paid to business continuity and recovery planning, in order to minimize the negative impact of successful attacks. Similar to the firm's cyber perimeter, these playbooks must be updated as needed based on changes to the firm's operations and the evolving cyber threat landscape.

3. Improve threat responses via cyber analysis and information sharing

Most common industry cybersecurity tools may be effective in addressing previously identified vulnerabilities, but they fall short in responding to threats in real time and anticipating future threats. To remedy this shortfall, a cyber risk monitoring team (often a sub-group of cyber risk operations) should collect and review intelligence from both internal and external sources to provide the firm's leadership with centralized, accurate, and timely risk analysis.

Timely exchange of cyber risk intelligence with peer institutions, regulators, and law enforcement agencies is a critical component of this effort which is yet to be successfully implemented across the industry (largely due to privacy and liability concerns). Nevertheless, financial institutions should utilize channels that promote information sharing, such as the ISAOs to be established by the President's recent executive order.

Additional information

For additional information about this **A closer look** or PwC's Financial Services Regulatory Practice, please contact:

Dan Ryan
Financial Services Advisory Leader
646 471 8488
daniel.ryan@us.pwc.com

Adam Gilbert
Financial Services Global Regulatory Leader
646 471 5806
adam.gilbert@us.pwc.com

Joseph Nocera
Financial Services Cybersecurity Leader
312 298 2745
joseph.nocera@us.pwc.com

Sean Joyce
Financial Crime Leader
703 918 3528
sean.joyce@us.pwc.com

Armen Meyer
Director of Regulatory Strategy
646 531 4519
armen.meyer@us.pwc.com

Contributors: Roozbeh Alavi, Douglas Roeder, Coryann Stefansson, and Grace Vogel.

To learn more about financial services regulation from your iPad or iPhone, click here to download PwC's new Regulatory Navigator App from the Apple App Store.

Follow us on Twitter @PwC_US_FinSrvcs