The Evolving Governance Model for Cybersecurity Risk

By Gary Owen, Director, Promontory Financial Group
Responsibility for the oversight of information security and cyber threats is moving from back-office technology professionals to boards of directors and corporate executives as it becomes increasingly clear that managing these risks across an organization demands involvement at the highest levels.

Companies in every industry confront mounting cybersecurity risks, but the threat to banking organizations is particularly significant. They are at the heart of an industry deemed critical infrastructure by the Department of Homeland Security, and their holdings of consumer data and dollars make them especially attractive to thieves and hackers.

The new governance model for information security and cybersecurity risk doesn't require the board and C-suite to become technology experts, but it does demand a cross-disciplinary approach — and the recognition that technology, while posing a significant risk, can also be a significant competitive advantage. Firms must update risk management skills to ensure technology risks and gaps are not only understood but also factored into decisions made by senior management. A well-protected organization is less likely to become a victim and stands to attract the customers of companies that do; it is also better-positioned to deliver services with effective and secure technology.

Firms that have not yet adjusted to the new cybersecurity risk paradigm typically have some common vulnerabilities:

- Boards of directors and executives that hesitate to engage on technology and cybersecurity issues,
- Risk management frameworks that don't capture the full range of technology risks, including exposure through vendors,
- Ambiguous lines of authority and a lack of accountability for protection, response, and recovery,
- Reliance upon security tools to respond to a crisis, rather than reliance upon front-end investments to prevent a crisis, and
- Inconsistent testing of their incident-response plans.

Competition for corporate time and resources is intense, but the financial and reputational damage
inflicted by security failures and data and privacy breaches is an enormous price to pay for taking partial measures. These breakdowns are often as devastating as failures in business, public relations, customer trust, and regulatory compliance.

How banking organizations should best address these risks varies by their size, complexity, and lines of business. Compared with community and regional banks, the largest banks have the obvious advantages that come with size: round-the-clock operations that can quickly address emerging threats, more employees dedicated to protecting against cybersecurity risk, advanced information-technology software and systems, and the capacity and scale to insource operations. But these resources must be deployed carefully to generate the greatest benefit. And of course, size comes with its own disadvantages, not the least of which is the greater number of threats large banks can expect to attract.

As the size of the organization decreases, generally so does the budget and staffing for managing cybersecurity risk. But while regional banks do not have the same flexibility that the largest banks have in deciding which activities to keep in-house, they usually have the advantage of being less technically complex. IT solutions and protection are commensurately less complex.

The tendency of regional and community banks to outsource the management of cybersecurity risks is a critical distinction from the largest banks. The Office of the Comptroller of the Currency (“OCC”) and the Federal Reserve Board (“Federal Reserve”) have separately issued guidance making it clear that banking companies retain the risk associated with outsourced activities. Banks must be able to clearly represent their controls and capabilities, regardless of who manages the implementation — which places a premium on competent vendor management. Managers must take an active role in evaluating the added risk or benefit of third parties, and continuously monitor the overall risk posture of the bank.

The common element for all banking companies — and indeed, all organizations — in managing cybersecurity risk successfully is a governance framework that suits their risk profile. Banks should identify where risk functions are managed and assess how much control they exert over those functions. That is a key element of the rationale for outsourcing, because whether to maintain a third-party relationship depends on an accurate assessment of the benefit of doing so. These decisions — which must be revisited on an ongoing basis — can't be made reliably unless banks' internal teams and third parties are reporting practical information that is used to make decisions about risk. This is especially pertinent as the OCC and the Federal Reserve each emphasized in its guidance the establishment and monitoring of performance standards for third parties.

Balancing Act

Many companies and directors don't always know where to focus time, attention, and resources, even though they have identified the pressing need to manage cybersecurity risk. That sense of urgency can lead to an uncalibrated response in which companies rush to prevent sophisticated attacks without first covering the basics. The result is similar to closing second-story windows without locking the front door.

Effective security is a balancing act to ensure the basics are covered while keeping an eye on what is around the corner. A good first step in undertaking significant cybersecurity programs is a sound governance model that addresses basic gaps and anticipates more sophisticated ones.
The program should also ensure that common vulnerabilities are addressed decisively.

**INSUFFICIENT BOARD AND EXECUTIVE ENGAGEMENT**

Organizations must maintain a strategic business focus on information security and cyber threats. Protecting the corporation's critical assets, including data and technology, is increasingly regarded as a fiduciary responsibility of the board. Yet technology disciplines are alien to many directors and executives, who were more likely chosen for their knowledge and experience in management, governance, accounting, or finance. The key is to approach technology-focused risk through the same prism as any other risk — that is, by insisting on having a clear and rigorous understanding of it and a process for managing it as other risks are managed. This means breaking through jargon and getting crisp responses to questions.

**INADEQUATE RISK MANAGEMENT FRAMEWORKS**

A formal risk management framework helps companies make decisions and set priorities about risk, and enables business lines and control and support functions to work together. Business units work to consistent standards, and support functions provide the same services and support regardless of location. In the absence of this type of framework, weak spots will emerge, without a clear line of sight from the corporate center. Boards and management should probe whether their risk management framework gives sufficient weight to technology and cybersecurity risk, as well as vendor relationships, which have been implicated in a number of cyberattacks. The organization should be able to profile its critical technological resources to understand what needs to be protected, recognize the threats to and vulnerabilities in those resources, adopt mitigation strategies, implement and continually test controls, and put in place a vendor risk management process.

**AMBIGUOUS LINES OF AUTHORITY AND A LACK OF ACCOUNTABILITY**

In an intrusion or other attack, who will be responsible for leading the team that addresses and resolves the matter? While there is no cookie-cutter answer to the question, neither the CEO nor someone in the IT department is likely to be the right person. The CEO has stature and breadth to lead the effort, but must maintain a higher strategic focus, while IT managers may have depth — but typically not the needed breadth across multiple disciplines.

**WHILE REGIONAL** banks do not have the same flexibility that the largest banks have in deciding which activities to keep in-house, they usually have the advantage of being less technically complex.

**CRISIS RESPONSE RATHER THAN FRONT-END INVESTMENT**

Companies that do not invest prudently in technology risk falling behind and exposing themselves to constantly changing cyber threats. It is critical for the board and management to forge a consensus on appropriate investment in cybersecurity risk protection, and follow through by budgeting appropriately. Front-end investments that are properly integrated within the IT framework prove to be far more effective than ad hoc expenditures on security tools purchased in response to a crisis.

**INCONSISTENT TESTING OF INCIDENT-RESPONSE PLANS**

A nimble reaction to a crisis requires having an incident-response plan, knowing where it is, and using it. Yet time and again, companies are caught flat-footed by breaches, attacks, and threats, and find themselves...
making up their plans as they go. While the ability to think on one’s feet is vital, a crisis should not mark the first time an organization or team exercises its incident-response plan. Companies can improve their response to future incidents through thorough planning and testing. The right response doesn’t start and end in technology. Engagement with business lines, operations, corporate communications, legal, executive management, vendors, partners, and other stakeholders is critical.

What Should Companies Do Now?

Companies’ overarching goals should be to assess, understand, and monitor threats; educate employees and clients; strengthen themselves before attacks occur; and improve their real-time response to threats, attacks, and intrusions.

RAISE BOARD AWARENESS

Foster understanding of cybersecurity risk through education. The board should know what questions to ask of management to ensure that it is safeguarding the company against cyber threats and attacks. Questions directors should be able to answer include:

- Who is in charge of information security? Who will lead incident response?
- What regular reports does the board use to track cybersecurity risks? How are incidents and threats reported, and at what point are they elevated to the board?
- Does the board include a director knowledgeable about cybersecurity? What is expected of the board in overseeing these risks? Which board committee takes the lead?
- Is the board informed about the most serious cybersecurity risks facing the industry, and has it worked with executives to develop a cybersecurity risk appetite statement?
- Does the company have a written cybersecurity risk management strategy and governance framework? How is it measured and how well is it working? When was it last reviewed?
- When was the last major incident? How was it resolved, what were the results, and what weaknesses, if any, were revealed? Most important, have weaknesses been addressed?
- What are the most likely types of external threats? What are the internal threats?
- What insurance policies cover the company against network security breaches and other cybersecurity incidents? Is this coverage up to date and is it adequate?
- Are all of the company’s information-security and risk management activities part of a defined and documented information-security program strategy?

THE COMMON element for all banking companies — and indeed, all organizations — in managing cybersecurity risk successfully is a governance framework that suits their risk profile.

ADDRESS ACCOUNTABILITY THROUGHOUT THE ORGANIZATION

The governance framework is the key to addressing accountability, but there are other important steps. Companies should assemble a cybersecurity team that includes representation from IT, the legal department, human resources, and public relations, at a minimum — and a designated leader to call the final shots. The CEO, with input from the board, should determine who the
Focused forward

At Key, our people share a set of core values that are essential to who we are and how we interact with our clients, communities, and each other. A vital part of these values is to take corporate responsibility seriously. We direct our time, expertise, and resources toward community and philanthropic investments, promoting diversity and inclusion, and driving sustainability.

These core values enable us to be **Focused forward** on our journey to create a top-tier organization that exceeds the expectations of our Corporate, Community, and Private Bank clients.

Visit key.com for more information.
A leader should be, taking into account the team’s mix of skills and experience.

**STRENGTHEN ENTERPRISE-WIDE RISK MANAGEMENT FRAMEWORKS**

Ensure that cybersecurity risk is monitored and addressed. Companies are already accustomed to mapping risks — whether in heat maps, spreadsheets, or other formats — to model and communicate risks visually and separate acceptable risks from unacceptable ones. Yet this process seldom extends to cybersecurity risk.

**COMPANIES THAT** do not invest prudently in technology risk falling behind and exposing themselves to constantly changing cyber threats.

**ASSESS CONTROLS AND COMPLIANCE WITH LAWS AND REGULATIONS**

The starting point is to understand the many regulations that address cybersecurity risk. Compliance can’t be verified through a once-a-year audit. Regulations, guidance, and the priorities of regulators change. Companies may be subject to multiple jurisdictions with overlapping or contradictory rules. Getting all teams working toward the same goal without interfering or duplicating activities guarantees efficiency while maintaining regulatory compliance and increasing regulators’ confidence in the organization.

**SCRUTINIZE VENDOR RELATIONSHIPS**

Vendors have access to important systems and data. This puts companies at risk of loss, manipulation, or theft of data that can expose external and internal relationships. Companies should be prepared to calculate the risk and necessity of current and potential vendors; adopt formal vendor-management policies and procedures; and train employees.

**ADOPT AND TEST THE INCIDENT-RESPONSE PLAN AT MULTIPLE LEVELS**

Every company should have an incident-response plan that can be put into action quickly in the event of a cyber threat or attack. Elements of this plan should include identifying team members to call upon in the event of a breach, detailing their roles, and establishing written protocols for determining how to inform clients, shareholders, regulators, and law enforcement. One of the most critical steps is to test the incident-response plan. Testing is the only way to determine whether the underlying assumptions of the plan will work in reality, and it gives incident-response team members much-needed practice in working together during a crisis.

**Conclusion**

Bolstering a company’s ability to withstand cyber threats and attacks requires a comprehensive response, including fostering board engagement, strengthening risk management, assigning managerial accountability, adopting and testing contingency plans, and making steady and appropriate IT investments.

Over time, companies should continue to improve their cybersecurity programs through sound risk management, continuing to raise the bar, expanding security tool and process coverage, refining security operations to be more efficient, and responding to new and emerging threats. Compliance with the rules is expected — but genuine security requires steady evaluation and alignment of the cybersecurity risk framework with the company’s business objectives, governance, risk management, IT, and regulatory considerations.

*Earl Crane, a senior principal at Promontory, contributed to this article.*