EVOLVING ROLE OF IA WITH CYBER RISK

BY BRIAN BROWNE

MAZARS

Cyber as an Organizational Risk

In 93% of data breaches, the targeted systems were compromised within minutes. 83% of the time, those breaches were not discovered for weeks, leaving the attackers with plenty of time to do their damage and exfiltrate data.[1] The average consolidated total cost of a U.S. data breach in 2016 was $7 million, and the average cost incurred for each lost or stolen sensitive data record was $221.[2]

The increasing digitization of corporate assets, the proliferation of network connectivity, the disappearance of distinct corporate borders, and the increasing motivation and capabilities of cyber adversaries have transformed cyber risk from a technical consideration for a single department into a significant business risk for the whole enterprise.

Board Cyber Risk Oversight

In response to the evolution in the complexity of cyber risk, the National Association of Corporate Directors (NACD) released the 2017 edition of their *NACD Director's Handbook on Cyber-Risk Oversight*. Their guidance consists of the following five key principles:

1. **Enterprise Risk** – Historically, cybersecurity has been considered an IT function; however, cyber risk oversight is a board-level responsibility, and directors need to approach it as an enterprise-wide risk management issue. Some of the highlighted areas for directors to engage management on include:

    - Crown Jewels – Management should have an understanding of the organization's most critical data assets - where they reside, how they flow through the organization, and who has access to them. This foundational understanding supports a focused and efficient protection and cyber risk reduction strategy. As part of this, management should consider not just high probability risks, but also low probability/high impact risks that would be catastrophic.
    - Third Party Risk – Management should understand cyber risks present not only within their own organization's infrastructure, but also within the larger ecosystem of partners, suppliers, affiliates, and customers within which it operates. The degree of connectivity that the organization has with third parties can increase its cyber risk exposure, as several well-known and significant breaches were initiated through third parties.

2. **Legal Implications** – The board and the individual directors should have an understanding of the cybersecurity legal and regulatory landscape that is applicable to the organization. This includes liability, public disclosure and reporting (e.g., SEC), information sharing, infrastructure protection, and data breach notifications. Some areas of emphasis for this principle:

    - Simulations/"Table Top" Exercises – As a result of the varied manners in which company executives have handled data breaches at their organizations, it has become clear that proper incident response planning is not just a necessity for IT staff and management, but also for corporate executives and directors. Corporate brands have been impacted by unclear and inconsistent executive communication. The Handbook recommends that directors participate in simulations or "table top" exercises to become familiar with their incident response procedures and communication approach.
    - Board Minutes – Formal Board meeting minutes should reflect when cyber risk issues are on the agenda or discussed, whether by the full board or key committees.

3. **Cyber Expertise** – While NACD research has shown that an increasing number of boards discuss cyber risk on a regular basis, it also indicates that most boards do not have an adequate understanding of it. In lieu of adding "single purpose" directors with cybersecurity expertise, boards can close this gap in other ways:

    - Deep dive briefings or examinations.
    - Leveraging existing independent advisors, such as external auditors and outside counsel.
    - Participating in director education programs.

4. **Cyber Risk Management Framework** – Directors should set the expectation that management will adopt an enterprise wide cyber risk management framework with adequate staffing and budget. This is important for every organization, but particularly for more distributed and decentralized organizations to establish a consistent approach to managing risk. The Handbook states that organizations should at least consider the adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

[1] 2016 Verizon Data Breach Investigations Report
[2] 2016 Ponemon Cost of Data Breach Study: United States

5. **Board-Management Cyber Discussions** – Alignment between board and management with respect to cyber risk should be obtained by having discussions of which risks to avoid, accept, and mitigate or transfer through insurance.

Three Lines of Defense, Internal Audit, and Cyber Risk

Although the NACD Blue Ribbon Commission on Risk Governance recommended that risk should be a function of the full board, research indicates that over 50% of boards assign cyber risk oversight to the audit committee. Given that this is where cyber risk governance discussions with management are occurring for many organizations, the role of internal audit to provide an independent and objective assurance of cyber risk management is critical.

The Institute of Internal Auditors (IIA) has defined this organizational cybersecurity role within their "Three Lines of Defense in Effective Risk Management and Control" model. Their Global Technology Audit Guide (GTAG) *Assessing Cybersecurity Risk: Roles of the Three Lines of Defense* identifies the owners and cybersecurity activities for each line of defense: management, risk and compliance, and internal audit.

As the third line of defense, the internal audit role is to independently assess cybersecurity risks and controls to ensure alignment with the organization's risk. This involves evaluating the effectiveness of cybersecurity controls in the first line of defense and reviewing the adequacy of cybersecurity frameworks, standards, risk assessments, and governance of the second line of defense.

Observations and Recommendations from the Field

Our experience in providing cybersecurity services to internal audit clients validates the increasing focus of boards and audit committees on cyber risk, and the increasing expectation that the internal audit function will provide appropriate coverage of cyber risk. This has been manifested in:

- Increasing audit committee reliance on existing providers such as external auditors and outside legal counsel.
- Increasing collaboration between the three lines of defense to obtain proper cyber risk coverage.
- An increasing percentage of cybersecurity related audits within the annual IT audit plan.
- A significant number of internal audit departments that achieve cyber risk coverage by leveraging the services of cybersecurity service providers.
- Depending on the overall organizational size and structure, there is sometimes a blurring between the second and third lines of defense, with internal audit assuming some of the more traditional second line functions in order to achieve appropriate organizational cyber risk coverage.

Some of the more typical internal audit cybersecurity coverage can be grouped into the following categories:

- Cyber Risk Management – A cyber risk management framework is a key governance component that enables an organization to evaluate organizational cyber risks to identify areas that need to be addressed either through mitigation or transference. There are different models, but most consider some sort of intersection of threats, vulnerabilities, and asset value to determine qualitative or quantitative risk. This is a strategic function that is intended to direct and evolve the organization's cyber protection efforts, and is typically a function of the second line of defense.
- Cyber Control Framework – A cyber control framework is a prioritized set of practices typically consisting of people, process and technology, that are intended to protect against an organization's cyber threats. The control framework can be continually adjusted to evolving risks through the cyber risk management process, and provides a link between risk management and operations. Internal audit coverage in this area can help answer common audit committee/board question, "Do we have the right controls in place to manage risk moving forward?"
- Technical Cybersecurity Assessments – These assessments are performed largely to identify current vulnerabilities within the IT infrastructure, and can include vulnerability assessments, penetration testing, web application security assessments, wireless security assessments, and social engineering. They are essentially point-in-time assessments that can help answer the common audit committee/board question, "What are our current cyber risks?"
- Cybersecurity Operations – Cybersecurity operations consist of the people, processes, and technologies that are in place to manage cyber risk within the IT infrastructure, and typically reflect the implementation of the cyber control framework. Examples of such operations include IT asset management, patch management, threat and vulnerability management, malware protection, logging and monitoring, and cybersecurity assessments. Depending on scope, an audit of the cyber control framework can provide some coverage of cybersecurity operations. However, some situations may warrant a deeper dive into a particular

operational area, such as the implementation of a new process or tool.

- Cybersecurity Compliance – Depending on the business and industry, an organization may have to comply with various governmental or industry regulations, such as FFIEC, HIPAA, and PCI DSS. Failure to comply with such regulations can result in considerable organizational impact - both direct ones such as fines and penalties, and indirect ones such as reputational damage. Internal audit coverage of these areas can provide an independent perspective on compliance, potentially identifying gaps that can be addressed prior to any regulatory body audit.
- Data Protection – A foundational issue for properly aligned cybersecurity is organizational knowledge of the entry points, flows, and storage locations of sensitive data. Such knowledge enables not only the implementation of direct protective controls, but also the prioritization of actions within the cybersecurity operations. Incorporating the processing or storage of sensitive data as an attribute within IT asset criticality supports prioritization of other actions such as patching, vulnerability remediation, and monitoring and response. Internal audit coverage within this area could include data classification, sensitive data inventory, data protection mechanisms such as access management and data leakage prevention (DLP), and IT asset management integration.
- Cyber Resilience – Internal audit functions have traditionally focused on preventive measures and controls. However, the increasing frequency and impact of data breaches and cyber incidents have shifted the cyber risk management paradigm to include quicker detection of incidents and breaches and effective organizational response. The internal audit function must mirror this paradigm shift in its cyber risk audit coverage to provide independent assurance and/or improvement opportunities in incident detection and response and, more broadly, cyber resilience.

An important consideration across all of these internal audit cybersecurity areas is for the Chief Audit Executive (CAE) to establish highly collaborative and productive relationships with the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) outside of the performance of cybersecurity related audits. This will promote the alignment of organizational cyber risk management views and help establish internal audit as a trusted cybersecurity advisor.

FOR MORE INFORMATION CONTACT:

BRIAN BROWNE, CISSP, CISA, CISM
PRINCIPAL
CYBERSECURITY SERVICES
+1 267.532.4368
brian.browne@mazarsusa.com

VISIT US AT www.mazarsusa.com

MAZARS