Deloitte.

Cyber security: The changing role of the Board and the Audit Committee

June 2016

www.deloitte.com/in
incicindia@deloitte.com

Introduction

Cyber security is among the most complex and rapidly evolving issues companies must contend with. With the advent of mobile technology, cloud computing, and social media, reports on major breaches of proprietary information and damage to organizational IT infrastructure have also become increasingly common, thus transforming the IT risk landscape at a rapid pace. Consequently, this has kept cyber security a high priority on the agenda of boards and audit committees.

- Organized crime is monetizing cyberspace, exploiting vulnerabilities in computer systems to compromise and remotely control computers; recording key strokes, monitoring screen displays and manipulating the computer user into divulging sensitive data.
- Cyberspace, being borderless, allows any attacker to route their assaults through multiple countries and jurisdictions, complicating investigation and law enforcement.
- Companies run the risk of losing substantial amounts of sensitive company information to malicious employees, who could also potentially remove it from company premises, or introduce malicious software to corrupt company databases or sabotage network operations.
- Corporate espionage by firms is commonplace in cyberspace. Attacks often target sensitive intellectual property, and there have been multiple instances of major firms with its security compromised over many months, losing substantial amounts of sensitive data during such attacks.
- Activism is also prevalent in cyberspace with sabotage and denial-of-service attacks growing progressively frequent. In the past, they would be attributed to 'hacktivist' groups such as Anonymous; but, increasingly, attacks point to political motivations.

What is the role of the Board and the Audit Committee?

Effective risk management is the product of multiple layers of risk defense. Business should support the board's need to understand the effectiveness of cyber security controls. Organizations should institute and continually shore up these three lines of defense:

Management

Companies that are good at managing information security risks typically assign responsibility for their security regimes to the highest levels of the organization. Management has ownership, responsibility and accountability for assessing, controlling and mitigating risks.

- Incorporate risk-informed decision making into day-to-day operations, and fully integrate risk management into operational processes
- Define risk appetite and escalate risks outside of tolerance
- Mitigate risks, as appropriate

Risk management and compliance functions

Risk management functions facilitate and monitor the implementation of effective risk management practices by management, and help risk owners in reporting adequate risk-related information up and down the firm

- Establish governance and oversight
- Set risk baselines, policies, and standards
- Implement tools and processes
- Monitor and call for action, as appropriate
- Provide oversight, consultation, checks and balances, and enterprise-level policies and standards

Internal audit

The internal audit function provides objective assurance to the board and executive management on how effectively the organization assesses and manages its risks, including the manner in which the first and second lines of defense operate. It is imperative that this line of defense be at least as strong as the first two.

- Independently review program effectiveness
- Provide confirmation to the board on risk management effectiveness
- Meet requirements of SEC disclosure obligations focused on cyber security risks

In absence of a competent and objective assurance, companies face the real risk of their information security and privacy practices becoming inadequate or even obsolete. This is a role that internal audit is uniquely positioned to fill. But to do so, it must have the mandate and the resources to match. For most organizations, information security and privacy are critical risks because of its potential to cause financial and reputational damage.

Given the recent high profile cyber-attacks and data losses, and the expectations of the SEC and other regulators, it is critical for the board to understand cyber risks.

The Board's role in Cyber Security

Cyber risk has become one of the top enterprise-wide risks facing companies. From a governance perspective, one of the board's most important tasks is to verify that management has a clear perspective of how the business could be seriously impacted, and that management has the appropriate skills, resources, and approach in place to minimize the likelihood of a cyber incident—and the ability to mitigate any potential damages.

Management's duty is to align the cyber risk program to a detailed business risk profile. When alignment is off, it's the board's duty to challenge management to construct a more tightly aligned program. In their oversight role, boards need to know the right questions to ask and how to monitor the effectiveness of management's plans and responses.

Such questions may include:

- Who is the appropriate executive to be leading cyber risk management?
- What are the greatest cyber threats our organization faces?
- What are the "crown jewels" that we must protect, including data and other assets?
- How will spending allow the organization to see and anticipate threats, and to quickly recognize when an attack has occurred?
- How will management's plan support the organization's ability to restore confidence after an attack, and minimize the business impact?
- Is cyber insurance appropriate, and if so, what type and level of coverage are needed, and at what cost?
- What is management's rationale for investing and allocating resources to monitor cyber risk, guard against it, and expedite response and recovery?
- How are we managing risk and ensuring that risk is reduced to an acceptable level?
- Have we identified vulnerabilities and gaps in preparedness, and how do we plan to improve the ability of management teams to make decisions under stress?
- What support is required from the board during a cyber incident or during crisis management?

As the board's role in cyber risk oversight evolves, the importance of a strong dialogue with management cannot be overestimated. Without close communication between boards and management, the organization could be at even greater risk.

The Audit Committee's role in Cyber Security

The extent of the audit committee's involvement in cyber security issues varies significantly by company and industry. In some organizations, cyber security risk is tasked directly to the audit committee, while in others, there is a separate risk committee. Companies, for which technology forms the backbone of their business, often have a dedicated cyber risk committee that focuses exclusively on cyber security.

Regardless of the formal structure adopted, the rapid pace of technology and data growth, and the attendant risks highlighted by recent security breaches demonstrate an increasing importance of understanding cyber security as a substantive, enterprise-wide business risk.

Audit committees should be aware of cyber security trends, regulatory developments and major threats to the company, as the risks associated with intrusions can be severe and can pose systemic economic and business consequences that can significantly affect shareholders.

Engaging in regular dialogue with technology-focused organizational leaders will help the committee better understand where attention should be concentrated. Some questions for audit committees to consider asking the management regarding cyber security:

- What is the overall strategy and plan for protecting assets?
- How robust are the organization's incident response and communication plans?
- What are the organization's critical assets and associated risks to be secured?
- How are vulnerabilities identified?
- How are risks disclosed?
- How are critical infrastructure and regulatory requirements met?
- What controls are in place to monitor cloud and supplier networks, as well as software running on company devices, such as mobile devices?
- What digital information is leaving the organization, where is it going, and how is it tracked?
- Do we have trained and experienced staff who can forecast cyber risks?
- Is it known who is logging into the company's network, from where, and if the information they are accessing is appropriate to their role?

Transforming Cyber Defenses

Cyber security is a business issue as it exceeds the boundaries of IT. Cyber risk needs to be managed with as much discipline as financial risk.

Both the technical nature of the threat and the amount of attention cyber risk demands calls for the board and the primary audit committee's involvement. Yet, organizations have acknowledged a lack of expertise on cyber security issues. As a result, boards and audit committees are not only seeking education for themselves, but also an elevation of the discussion amid C-level executives. These efforts include increasing engagement with the chief information officer (CIO) and the chief information security officer (CISO), drawing on the expertise of the IT partner from the external audit firm, encouraging CIOs and CISOs to participate in peer-group information sharing, and challenging management to produce metrics that the audit committee can use to evaluate cyber security effectiveness.

A comprehensive cyber security plan also requires an appropriate culture and tone at the top. These encompass an awareness of the importance of security extending from the C-suite to the professionals in each function, since breaches can occur at any level and in any department.

The CEO should make it clear that cyber security is a major corporate priority, and should communicate that he or she is fully committed to enforcing compliance with policies, and supporting efforts to strengthen infrastructure and combat threats.

Several practices that companies are employing to enhance the board and the audit committee's oversight of cyber security risk, leverage the recent broader strategic focus of the CISO and CIO roles:

- Increasing interaction with the IT department
- Sharing information with industry counterparts
- Technology experts joining the board
- Engaging the expertise of the external audit firm
- Deploying internal audit
- Evaluating the company's cyber security program

Throughout the past decade, most organizations' cyber security programs have focused on strengthening prevention capabilities based on established information assurance strategy: defense in-depth. This approach advocates a multi-layered approach to deploying security controls with the intent of providing redundancy in the event a security control fails or a vulnerability is successfully exploited in one of the layers.

To be effective and well balanced, cyber-defense must be secure, vigilant, and resilient.

Secure: Being secure means focusing protection around the risk-sensitive assets at the heart of your organization's mission—the ones that both you and your adversaries are likely to agree upon are the most valuable.

Vigilant: Being vigilant means establishing threat awareness throughout the organization, and developing the capacity to detect patterns of behavior that may indicate, or even predict, compromise of critical assets.

Resilient: Being resilient means having the capacity to rapidly contain the damage, and mobilize the diverse resources needed to minimize impact—including direct costs and business disruption, as well as reputation and brand damage.

Actionable threat intelligence

Strategic organizational approach

Looking Ahead

As recently as five years ago, it was rare for board of directors to be closely involved in managing cyber security risks, but rapid advancements in technology, coupled with a corresponding increase in the sophistication of cyber criminals and cyber legislation, have made it essential for the board and the audit committee to be informed and proactive. New technologies continue to shape the physical and virtual borders of organizations, which must frequently review and quickly adapt policies to address emerging issues.

Cyber security specialists are developing increasingly sophisticated approaches for preventing, detecting, and responding to security breaches, but no single solution can address all the evolving challenges associated with cyber threats. It remains important to apply prudent and adaptable controls to respond to changes in the threat landscape, and to have strong response and resiliency plans in place in the event of an attack.

Increasingly, cyber security is becoming a top-of-mind issue for most CEOs and boards, and they are becoming more preemptive in evaluating cyber security risk exposure as an enterprise-wide risk management issue, not just an IT concern.

Key contacts – India

Amry Junaideen,
President
Enterprise Risk Services
amjunaideen@deloitte.com

Shree Parthasarathy,
Partner and National Leader
Cyber Risk Services
sparthasarathy@deloitte.com

A.K. Viswanathan,
Partner
Enterprise Risk Services
akviswanathan@deloitte.com

Priti Ray,
Partner
Enterprise Risk Services
pritiray@deloitte.com

Maninder Bharadwaj,
Partner
Enterprise Risk Services
manbharadwaj@deloitte.com

Abhijit Katkar,
Partner
Enterprise Risk Services
akatkar@deloitte.com

Ashish Sharma,
Partner
Enterprise Risk Services
sashish@deloitte.com