

Audit Committee *Brief*



Cybersecurity is among the most complex and rapidly evolving issues with which companies must contend. Reports of major breaches of proprietary information and damage to organizational IT infrastructure have become increasingly common in recent years, and developments in mobile technology, cloud computing, and social media continue to alter the IT risk landscape.

A recent study¹ by the Ponemon Institute found that among companies surveyed between 2010 and 2012, the number of successful attacks on organizations per week more than doubled, and the financial impact of the attacks increased by nearly 40 percent. Such attacks can negatively affect market positioning if the public's confidence in the security of information and access to services is shaken.

In addition, regulators continue to carefully evaluate cybersecurity issues. In a May 2013 letter to Senator Jay Rockefeller (D-WV), SEC Chairman Mary Jo White said the SEC's staff was reviewing compliance with current [disclosure guidance](#) regarding cybersecurity for public companies to determine its effectiveness and whether further action is required.

The audit committee plays a vital role in monitoring management's preparation for and response to cyber threats and the associated regulatory and business developments.

¹ [2012 Cost of Cyber Crime Study](#) (Ponemon Institute, sponsored by HP Enterprise Security)

Questions for audit committees to consider asking management about cybersecurity:

- 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, and 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?

What are the most common types of cyber attacks, and what is their source?

There are numerous categories of cyber attacks and a variety of corresponding motivations, including financial fraud, information theft or misuse, activist causes, attempts to render computer systems inoperable, and efforts to disrupt the critical infrastructure of government and its vital services. The perpetrators of cyber attacks can range from individuals or small-scale operations such as insiders, suppliers, and activists, to large-scale, organized efforts perpetrated by criminal networks and foreign governments. Common modes of attack include the introduction of malicious software such as trojans, worms, viruses, and spyware; password phishing; and denial-of-service attacks intended to crash websites.

Each type of attack presents unique challenges and requires a targeted set of prevention activities, not all of which are related to technology. Phishing or social engineering techniques, for instance, are often dependent on employees divulging their password or other sensitive information when requested under false pretenses. Thus, education and awareness across the organization of policies and the reasons behind them are of paramount importance in preventing losses.

Organizational roles and responsibilities for cybersecurity

Audit committee and board of directors – Overseeing a successful program of cybersecurity requires frequent and proactive engagement from the board of directors and audit committee. The audit committee, in its capacity of overseeing risk management activities and monitoring management's policies and procedures, plays a significant strategic role in coordinating cyber risk initiatives and policies and confirming their efficacy. These responsibilities include setting expectations and accountability for management, as well as assessing the adequacy of resources, funding, and focus for cybersecurity activities. The audit committee chair can be a particularly effective liaison with other groups in enforcing and communicating expectations regarding security and risk mitigation.

Boards are devoting increased attention and resources to responding to cybersecurity issues. In a recent study² of global enterprise security governance practices conducted by the Carnegie Mellon University CyLab, 48 percent of corporations surveyed reported having a board-level risk committee responsible for privacy and security risks, a dramatic increase from the 8 percent that reported having such a committee in 2008. Forty percent of North American respondents indicated that their company's board deals with computer and information security issues.

² [Governance of Enterprise Security: CyLab 2012 Report](#) (Carnegie Mellon University CyLab)

Tips for enhancing cybersecurity governance

- Focus on controls for the most critical data areas; clarify the impact on the business and what will be done in the event of an incident.
- Evaluate the cyber incident response plan. Understand where vulnerabilities have been identified and the steps that have been taken to mitigate such concerns. Look for areas of consistent weakness in controls.
- Security budgets can at times be neglected in favor of other IT or business priorities; therefore, it can be helpful to annually review cybersecurity budgets.
- Require regular reports from senior management on privacy and security risks based on key risk indicators rather than on project status. Solicit metrics that help quantify the business impact of cyber threat risk management efforts.
- Work with internal and external specialists to stay apprised of recent developments in technology and cybersecurity. The audit committee should be briefed on all significant emerging issues.
- Confirm that privacy and security requirements for vendors, including cloud, mobile, and hosting providers, comply with the company's security program, including security control requirements. Carefully review notification procedures in the event of a breach or security incident.
- Conduct an annual evaluation of the use of and need for cyber insurance.

Whether or not there is a dedicated risk committee on the board, it is important to confirm that there are directors with security, IT governance, and cyber risk knowledge and skills. Given the audit committee's responsibility for risk oversight, it can be advantageous to recruit committee members with cybersecurity experience so that informed decisions can be made about the sufficiency of the efforts overseen.

Management – All members of management should be fully aware of the plan of action and who will occupy key roles in the event of an attack or threat. Most companies have in place a senior management position related to information security so that there is a clear voice directing cyber threat prevention, remediation, and recovery plans, related educational activities, and the development of frameworks for effective reporting. This position is sometimes held by a chief information officer, or a chief security officer who is also responsible for physical security, but some companies may have a dedicated chief information security officer who focuses solely on cyber threats. These executives will sometimes report directly to the board, but in all cases, they can be an effective liaison with whom the audit committee and board can communicate regarding risks and the response to attacks.

Internal audit – The audit committee should confirm that the internal audit function regularly reviews controls pertaining to cybersecurity, is up to date on the latest developments, and includes related issues prominently and regularly on its agenda.

External auditor – The external auditor can often be a valuable source of information on cybersecurity issues. Many firms have practices focused on evaluating and strengthening security controls and on implementing programs for enterprise risk management, and can share perspectives gained through working with a wide variety of companies in diverse industries.

External specialists – It can be helpful to seek the input of external specialists in assessing cybersecurity. Companies can conduct annual outside reviews of security and privacy programs, including incident response, breach notification, disaster recovery, and crisis communication plans. Such efforts can be commissioned and reviewed by the board's risk committee or another designated committee to confirm that identified gaps or weaknesses are addressed. Third-party security assessments can also provide benchmarking relative to other companies of similar size or in the same industry.



Executive order on cybersecurity

Concern regarding the extent to which cyber threats can undermine the capital markets, compromise sensitive information, and threaten vital infrastructure has reached the highest levels of government. In February 2013, President Obama issued an [executive order](#) to examine the development and implementation of risk-based critical infrastructure standards through a public-private collaboration that features mutual information sharing. The goal is to build a voluntary cybersecurity framework that helps “maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”

The National Institute of Standards and Technology (NIST), which has been charged with developing the framework, issued for public comment in February 2013 a request for information in association with the project. According to the NIST’s recently released [analysis](#) of the comments received, the issues most frequently raised included approaches to risk management, understanding the threat environment, cyber risk in the context of business risk, industry best practices, and impact on global operations. The NIST held a series of workshops in association with the project and issued a [draft outline of the preliminary framework](#) on July 1, 2013.

The [June/July 2013](#) issue of the *Audit Committee Brief* highlights the importance of audit committee members understanding and being involved in the changing rule-making landscape.



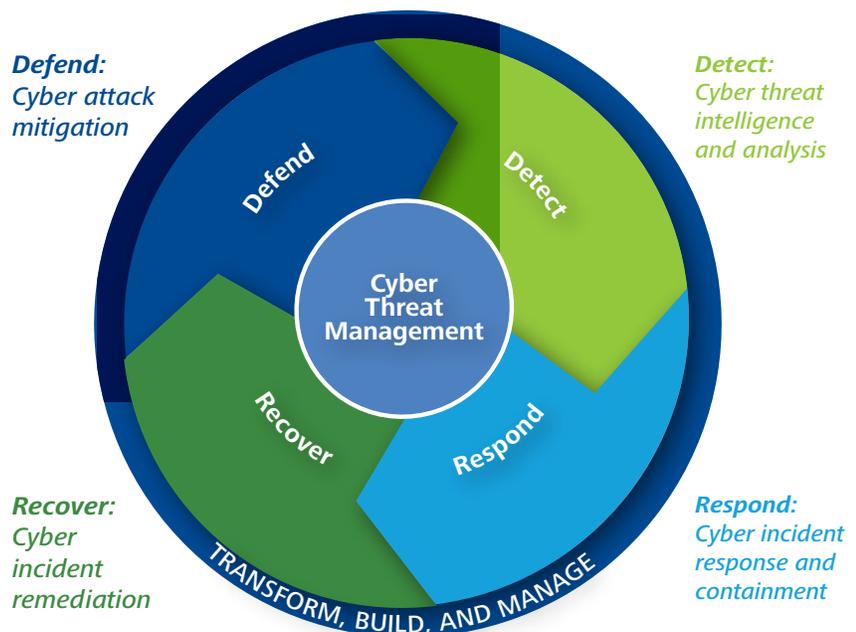
Building an effective cybersecurity plan

An effective cyber threat management plan recognizes and accounts for the four major phases of cybersecurity:

1. Cyber threat defense and mitigation
2. Threat detection, intelligence, and analysis
3. Cyber incident response
4. Incident remediation and recovery

Large companies can experience dozens of thwarted or successful cyber attacks in a year, and thus a fully realized response will operate under the assumption that there will be attacks and that some may be successful to at least a certain degree.

A comprehensive cybersecurity plan requires the appropriate culture and tone at the top, which includes an awareness of the importance of security that extends 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 cybersecurity is a major corporate priority, and should communicate that he or she is fully on board with enforcing compliance with policies and supports efforts to strengthen infrastructure and combat threats.





Visit the [Center for Corporate Governance](http://www.corpgov.deloitte.com) at www.corpgov.deloitte.com for the latest information for boards of directors and their committees.



To subscribe to the *Audit Committee Brief* and other Deloitte publications, go to <https://deloitte.zettaneer.com/subscriptions>.

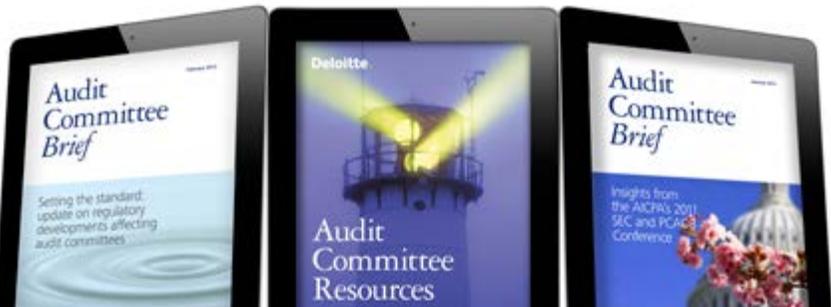
Conclusion

As recently as five years ago, it was rare for boards of directors to be closely involved in managing cybersecurity 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 audit committee to be informed and proactive. New technologies continue to shape the physical and virtual borders of organizations, and organizations must frequently review and quickly adapt policies to address emerging issues.

Cybersecurity 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.

Now you can instantly access the *Audit Committee Brief* through a free, easy-to-use tablet app. Deloitte's Audit Committee Resources application is available in the iTunes App Store. New issues of the brief are made available for download each month and feature useful multimedia content not available in the print version. The application also includes an interactive edition of the popular *Audit Committee Resource Guide*.

Click [here](#) or visit the App Store and search for "Deloitte Audit Committee Resources" to download the application.



This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser.

Deloitte is not responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte LLP and its subsidiaries. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Member of Deloitte Touche Tohmatsu Limited