Cybersecurity
Considerations for the audit committee
2012 Global Information Security Survey
Many organizations are taking steps to enhance their information security capabilities, but few are keeping up with an ever-changing risk landscape. Find out more at ey.com/giss2012
Virtualization, mobilization and cloud technology have created new points of entry into businesses, leaving them vulnerable to covert cyber attacks. Many companies already have been breached, but not all of them know about it. Executives at many organizations say it’s a struggle to contain the threats, and nearly impossible to thwart them.

Ernst & Young interviewed more than 1,800 information security executives for the 2012 Global Information Security Survey, and 77% of them indicated an increase in external threats. Despite the enhancements companies have made, there is a gap between where security is and where it needs to be. Boards of directors are starting to take note, particularly members of the audit committee, who list cybersecurity among their top concerns.

As technology continues to evolve, the benefits increase — and so do the risks.

Boardroom attention

Information technology (IT) is often a high-level agenda item discussed at least annually in most boardrooms. However, high-profile cases, such as the alleged Iranian attack against US banks1 and a resurgence of attacks on US companies from Chinese hackers2 have shifted the IT conversation to cybersecurity and data protection, as well as made these discussions more frequent.

Cybersecurity is not just a technology issue; it’s a business risk that requires an enterprise-wide response. Yet only 38% of the executives who responded to the recent survey said they align their information security strategy to the organization’s risk appetite and risk tolerance. Effective information security transformation requires leadership, commitment and the capacity to act.

Getting up to speed

Most audit committee members are financially savvy, but they may lack a deep knowledge of technological issues. They therefore rely more heavily on the technology officers within the company to provide them with perspectives on IT risk management. Still, only 54% of survey respondents said they discuss information security in the boardroom quarterly or more frequently.

While technology officers are able to provide data, such as the number of attempted breaches, it can be difficult to convert the data into meaningful information that could help audit committees and boards better understand the possible risks facing the entity. On top of that, board and audit committee members may not know how to evaluate the quality of the information they receive or ask the right follow-up questions.

Uncertainty can lead to hesitation, and inaction can damage the company’s brand and reputation, disrupt business continuity and lead to a host of financial and legal ramifications.

Like the technology itself, the financial consequences of a cyber attack are often not well understood. Theft of funds and intellectual property is not the only risk. There are costs associated with losses of profits and business as well as the expenses associated with remediation. A breach eventually could affect financial performance, ultimately reducing earnings per share and the company’s overall market value.

Uncertainty can lead to hesitation, and inaction can damage the company’s brand and reputation.
The benefits and risks of new technology

The financial crisis has placed pressure on businesses to cut costs where they can, and technology helps streamline the process. But the same technologies that propel businesses forward are the ones creating new risks.

Companies want to increase operational flexibility, and 59% of those who responded to the Ernst & Young survey said they have moved to the cloud or plan to do so. However, 38% of those moving to the cloud indicated that they haven’t done anything to mitigate the potential risks inherent in the cloud, such as legal, regulatory and compliance risks around data privacy. The majority of those who have taken measures are employing encryption techniques and stronger oversight of the contract management process for cloud service providers.

Social media is another method companies use to enhance their brand by interacting with customers. The around-the-clock availability means that it can take little time or effort to damage a company’s reputation. Challenges include data security, privacy concerns, regulatory compliance and concerns about employees’ use of work time and equipment to engage in social media. Thirty-eight percent of the companies represented in the survey don’t have a coordinated approach to social media usage within or by the organization.

For many companies, mobile technology goes well beyond cell phones. Tablet computer use has more than doubled since 2011, with 44% of survey respondents now allowing company or privately owned tablets. Thirteen percent support the use of privately owned tablets through a “bring your own device” policy. As employees spend more time away from the office, the dramatic increase in the flow of information in and out of the organization becomes tougher to control. But fewer than half of the organizations surveyed use encryption techniques to protect their information while tablets are in use.
Whose job is it?

An effective security strategy needs to work in tandem with different functional areas. In the 2012 survey, 63% of the participants said the IT function is responsible for information security efforts. Twenty-six percent have made the CEO, CFO or COO responsible, making it a C-suite issue. But only 5% have given the task of information security to the chief risk officer, the person most responsible for managing the organization's risk profile.

While external threats ranging from “hacktivism” and state-sponsored espionage to organized crime and terrorism continue to increase, so do instances of internal vulnerabilities. Inadvertent data loss is escalating, whether the source is a careless worker or a disgruntled former employee. Thirty-seven percent of those who responded to the survey said careless or oblivious employees were among the threats that had most increased their enterprise’s risk exposure.

Organizations must go beyond protecting the perimeter. They should also focus on protecting the data itself. It will take money and resources to train employees across the enterprise to keep information safe. However, only 22% of respondents said they plan to spend more on cybersecurity in the next 12 months.

Putting the right processes in place would be a big step forward. However, the majority of organizations represented don’t have a structured, effective framework for assessing and managing security risks. Instead, they indicated they rely on a patchwork of non-integrated, complex and fragile defenses. Sixty-three percent of respondents don’t have a formal security architecture framework in place, and they don’t plan on using one. Only 56% conduct penetration tests, and 19% fail to test at all.

---

The company’s board should set the tone for enhancing security and determine whether the full board or a committee should have oversight responsibility. In some cases, a risk committee, executive/operating committee or the audit committee will be given the oversight charge.

Some audit committees may need better information about the company’s processes, and they should leverage that information to understand what oversight is necessary. They should understand whether management has the right people and processes in place. The audit committee’s action plan will depend on the company’s level of maturity in managing security risks, and it may require more attention and time in sectors where these risks and the potential for damages are highest, such as financial services institutions. Depending on the circumstances, some boards of directors may want to consider bringing someone with a deep understanding of IT issues onto the board or audit committee.

Audit committees should ask questions about the state of specific security programs and then ask for benchmarks: how is the company doing relative to its competitors and the industry? They should also ask for an explanation of the measures that are in place to prevent or detect attacks. It’s important to gauge the pulse of the company’s tolerance for risk and evaluate the decisions made by management over which gaps are tolerable.

What is your role?

Questions for the audit committee to consider:

- Has the company experienced an increase in the number of information security breaches?
- What has the company done to bolster its information security program?
- Is information security an IT function within the company? If so, to whom does it report?
- Is there anyone on the audit committee or on the board with an IT background?
- Is the audit committee involved in planning for better management of information security risks?
- How often does the committee discuss cybersecurity? Who presents that information to the board?
- Does the audit committee seek or receive routine updates on risks and advancements in information security?
Ernst & Young

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 167,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

©2013 Ernst & Young LLP.
All Rights Reserved.

SCORE no. GA0001
BSC no. 1303-1046255

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither Ernst & Young LLP nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

ED 0114