NYSE Governance Services

NYSE

Managing Cyber Risk: Are Companies Safeguarding Their Assets?

RSA

In the last few years, companies both in the United States and abroad have witnessed the steady growth of cyberattacks and corporate espionage. The financial losses and, worse, often irreparable reputational harm such incidents wreak have served to place a target squarely on the backs of board members to ensure they are properly overseeing cyber risk.

To get a better grasp on how U.S. boards are handling cybersecurity roles and responsibilities, NYSE Governance Services, Corporate Board Member and RSA, in association with EY, surveyed more than 200 audit committee members this spring on a variety of issues regarding their cyber risk oversight program. This paper will outline the top-line issues surrounding cyber risk oversight and highlight the findings of our study on directors' opinions related to their role in cyber risk oversight.

The landscape for cyber risk today

Cybersecurity risk is increasing in every measurable dimension. According to research from Akamai Technologies, a leading provider of cloud services with more than 150,000 servers in 92 countries, during the fourth quarter of 2013, its customers were targeted by 346 DDoS (distributed denial of service) attacks, 23% more than in the prior quarter, and nearly 75% more than in the fourth quarter of 2012. Observed attack traffic in the United States increased from 11% in the third quarter of last year to 19% in fourth quarter 2013.

Furthermore, in March of last year, U.S. intelligence leaders said for the first time that cyberattacks and espionage have eclipsed terrorism as the top security threat facing the country. Cybersecurity bills have been introduced at the federal level in both 2012 and 2013, but so far, no law has been enacted. The SEC issued voluntary guidance in 2011, but since the guidance held no new requirements, the effort has had little impact, experts say.

"There's a good reason we haven't seen new requirements," says Erica Salmon Byrne, executive vice president of Compliance & Governance Solutions, NYSE Governance Services, an Intercontinental Exchange company. "The challenge will be how much—and how often—to disclose." Technology is changing at a faster and faster pace and companies are trying hard to keep up, which could put organizations in the position of having to constantly update disclosures as processes are improved. There are also many companies for whom security protocols are a competitive advantage, and disclosure would be problematic for them.

Loss severity is also increasing. As noted in *Corporate Board Member* magazine's May issue, the average annualized cost of cyber breaches is $11.6 million per year per company, according to Ponemon Institute's 2013 Cost of Cyber Crime Study, with a range of $1.3 million to $58 million. 2012's average annualized cost was $8.9 million, a difference of $2.7 million, which translates to a 30% increase, Ponemon's study notes. The 60 U.S. companies included in the study experienced 122 successful attacks per week and 2.0 successful attacks per company per week (a nearly 20% increase over last year's successful attack experience), which doesn't take into account the plethora of attempted intrusions turned away by company firewalls. Furthermore, losses in the United States are especially acute, with the U.S. leading nine other nations in average total organizational cost per breach and, along with Australia, the largest average number of breached records, according to Ponemon.

"The cybercrime world is like an arms race," says Amit Yoran, senior vice president of RSA. "Cybercriminals pursue a course of action until the defenders work out how to combat it, at which point the cyber criminals change tack." RSA's approach is to implement an intelligence-driven security model, focusing on visibility and analytics. The result is agility rather than simple point controls, which continue to be bypassed, says Yoran.

In addition, the proliferation of social media in the corporate world has resulted in increased risk. Despite the many unknowns about this relatively new phenomenon, two-thirds of the directors we surveyed said their board only occasionally discusses social media, and 17% said they never discuss it.

"Corporate executives need to be aware of the company's social media presence. Beyond marketing, HR, or service operations, social media platforms

provide immediate customer feedback that can be a PR issue. We've also seen social media be used to manipulate markets with tweets presenting misinformation about corporate transactions or current events," says Julie A. Bernard, principal, Advisory Services, Ernst & Young LLP. "From an awareness point of view, directors need to understand how their own public presence—on social media or other news coverage—may impact the institution's cyber risk, even if it's not their intent. Reputations were difficult to manage before social media; now challenges are immediate," she says.

According to a 2012 report by the SANS Institute, a cooperative research and education organization and one of the largest sources of information security training, some of the risks an organization should consider with regard to social media usage include compliance with regulatory requirements, reputational damage, information leakage, loss of intellectual property, malware attacks, copyright infringement, and privacy breaches.

The role of the board

In today's ubiquitous digital world, IT/cyber security is an enterprisewide, strategic risk issue requiring ongoing board oversight. Although experts agree the day-to-day management of cyber and social media risk should be undertaken by the executive leadership team in tandem with the IT department, it is still up to board members to ensure they can properly discuss the implications of such risks on the company and on shareholder value.

According to Salmon Byrne, cyber risk is just the latest risk board members must address, and good directors are doing so in the context of the company's overarching risk management process. "Breach plans, drills, and testing protocols are the responsibility of the IT team and leadership team, but directors must be quizzing leadership on how they are approaching cyber risk and where it fits into the company's risk profile. Without that, the board isn't fulfilling its obligation to shareholders," she says.

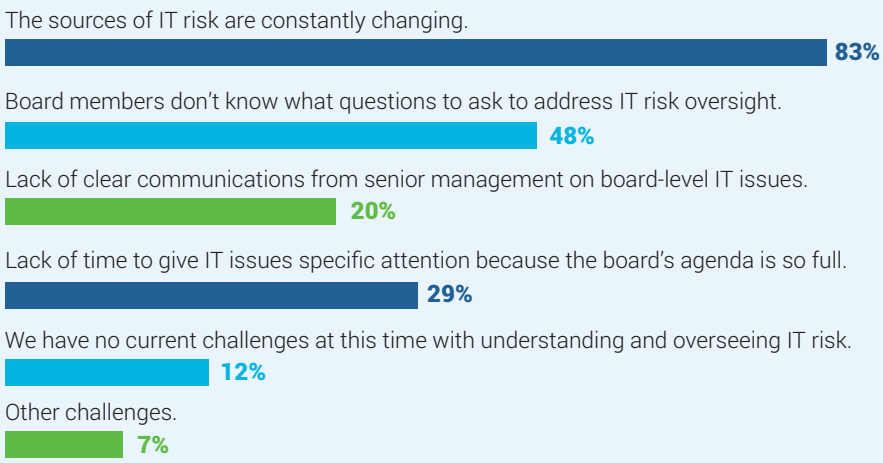
Figure 1

To what extent do you agree or disagree with these statements related to your company's IT risk oversight?

	Agree	Somewhat Agree	Somewhat Disagree	Disagree	Unsure
Our company has IT risk very well under control with regard to the possibility of a cyber breach.	20.77%	58.45%	10.14%	5.80%	4.83%
To make sound decisions related to IT risk oversight, it is necessary for companies today to have at least one board member with a specific IT background.	24.64%	33.82%	25.60%	14.98%	0.97%
Our board has one or more members who do not have the skills and understanding of IT risk to provide effective oversight in this area.	32.20%	28.29%	18.54%	17.07%	3.90%

Figure 2

Which of the following present challenges for your board's oversight of IT risk? *(Select all that apply.)*



In a marked turn from just a decade ago, our survey found the majority of directors believe that IT/cyber expertise within their ranks is needed. Nearly 60% of directors from our survey believe having at least one board member with a specific IT background is necessary to help make sound decisions related to IT risk oversight (Figure 1). Admittedly, changes in board composition happen

slowly, so it's no surprise that about 60% of directors are worried they may have board members who are incapable of providing effective oversight of IT/cyber risk.

Digging a little deeper, we asked directors to choose from among several challenges they currently face with regard to their effective oversight of IT/cyber risk (Figure 2). Eight out of 10 respondents (83%) stated that the biggest challenge is the fact that the sources of risk are constantly changing. In addition, almost half of directors (48%) worry they don't know enough to ask the right questions.

"Adding IT expertise to the board is a good talent diversification strategy that helps address the knowledge gap among directors. Yet the more complex board challenge that remains is the difficulty of quantifying cybersecurity risk and determining 'How much is enough?'" Ernst & Young's Bernard says. Having additional expertise on the board, as well as qualified outside consultation, may help companies with some of these more difficult risk decisions.

Developing a strategic approach

Looking at the big picture, corporate directors may well feel as if bulletproof oversight of cyber risk is impossible. Knowing how difficult it is to protect the company from every possible risk scenario, a sound approach is to evaluate which of the company's prime assets or transactions are most valuable—and thus most vulnerable—and to roll out a risk management strategy accordingly.

Stated another way, there are multiple jewels in every company's crown, but not all of them are mission critical or set the business apart as unique. For some, the jewel might be a proprietary database, a chemical formula, a patented manufacturing process, or other type of intellectual property. It could be your customers' private financial data or competitive research that has been years in the making. Any of these, if stolen or otherwise compromised, could send a company on a downward spiral overnight, resulting in regulatory investigations, litigation, and loss of shareholder value. Therefore, the first step is to undertake a thorough analysis of these trophy assets and determine the risk that each might present in the event of a cyber breach or loss.

"Increased threats, stagnant budgets, and increased complexity require prioritization of efforts to protect organizational data. Perceived threats—what an attacker would target—can serve as a framework for focusing protection efforts," explains Bernard. EY's Differentiated Asset Protection approach, for example, identifies the most critical security assets (e.g., confidentiality, integrity, availability), and then guides the selection and controls the effectiveness and cost of additional security controls to be applied to the assets. "This approach uses key steps to effectively identify a small number of critical assets and strengthen their controls," Bernard adds.

With an undertaking of this magnitude, boards today should work in tandem with executive management on this type of approach. In the past, companies and boards may have assigned IT risk management to the IT team. But increasingly, the board and C-suite should look at the oversight and management of such risk as a strategic exercise, including the evaluation and prioritization of trophy assets, thus allowing the company to assign resources and employ proactive oversight in a more effective manner.

Figure 3

How confident are you in your management's ability to respond to and mitigate the scope of IT/cyber threats in the current envvironment?

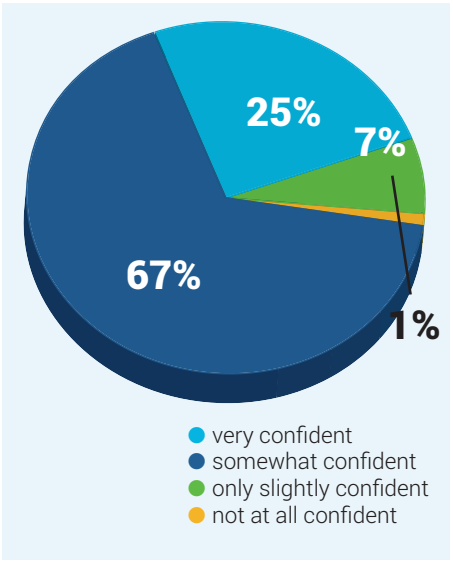
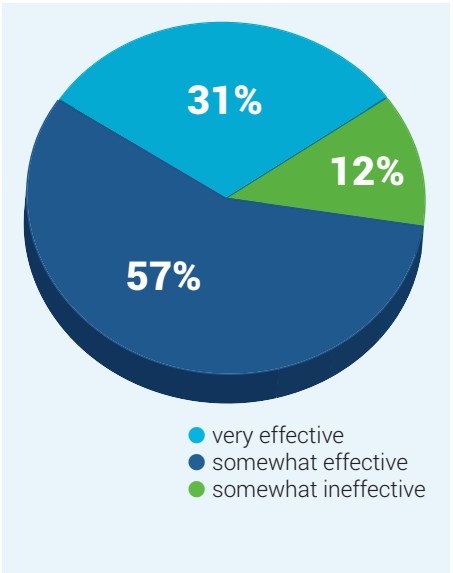


Figure 4

How effective is your board at holding management accountable for managing cyber security risk?



Often however, setting up good communications presents its own challenges. The key to an effective board/management partnership on cyber risk is maintaining ongoing lines of information—both in and out of the boardroom. Just as with other aspects of corporate oversight, whether it concerns internal audit, the legal department, or investor relations, boards must develop strong, effective communications with IT executive management to stay abreast of key issues. Increasingly today, CIOs and CTOs are becoming members of the executive team where they play key roles in corporate strategy as well as risk management. One benefit, say IT experts, is that once the these lines of communication and reporting are developed, potential problems will be caught earlier and addressed in a manner that helps ensure the company doesn't make the same mistakes twice or in separate silos of the organization.

"Perhaps instead of worrying too much about reporting on a metric, boards should be evaluating their security teams on their ability to change tactics to respond to new threats," says George "Chip" K. Tsantes, principal, Advisory Services, Ernst & Young. Essentially, Tsantes says, this means be ready to make and respond to new mistakes. "Cyber incidents, and every organization has them, should be different each time. If the same incident occurs multiple times, people are not implementing proper controls, technology, and awareness to learn from past incidents."

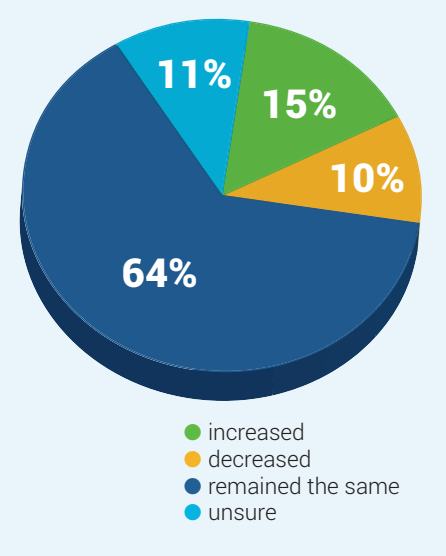
Room for improvement

Our survey asked several questions designed to ferret out directors' opinions on how well they feel they are doing with regard to IT/cyber risk oversight. The survey found that only 21% of directors agree that their company has IT risk well under control with regard to a possible cyber breach; the majority (58%) offered a more tepid "somewhat agree" when asked, and 16% disagree to some degree. Moreover, only a quarter of directors surveyed are quite confident in management's ability to respond to and mitigate the scope of a cyber security threat (Figure 3), perhaps in part because about two-thirds said their senior IT executive reports to the board only "occasionally." By the same token, just over 30% find the board "very effective" at holding management accountable for managing cyber security risk, while the majority (57%) rate the board only "somewhat effective" (Figure 4).

Lack of budget, personnel, and tools were noted by roughly a third of respondents as current challenges to the effective operation of the information security function within their company. When allocating resources across the enterprise, Ernst & Young's Bernard cautions that companies need to balance initiatives that are revenue generating and those that involve managing risk. "Without a reasonable quantification mechanism, cybersecurity initiatives will consistently lose on an ROI basis. This leaves IT risk professionals backed into a corner and left with fear, uncertainty, and doubt to promote their programs," she says.

Interestingly, most directors surveyed believe the incidence of damage related to cybersecurity at their company has remained the same (64%); only 15% said it has increased. Eleven percent confessed they were unsure of the numbers for their company (Figure 5). Yet EY's Global Information Security data points to higher levels of reported damage incidence, perhaps indicating a communications disconnect between companies' boards of directors and their security teams.

Figure 5
Over the last year, has the incidence of damage related to information/cybersecurity at your company:



Overall, industry data shows global cyber risk is growing both in scope and severity, yet the survey demonstrates that in practice, boards are not always addressing it as a top priority. Indeed, when asked how often the board discusses topics related to risk and enterprise value, 42% admitted their board only occasionally discusses cyber/IT security (Figure 6).

In terms of its priority as an agenda item, just under half of the directors we surveyed said IT/cyber risk is discussed as a separate, full-board agenda topic. Thirty-eight percent said it is addressed by a separate risk committee, with recommendations later taken to the full board. As with many aspects of governance, one size does not fit all regarding how a company's board decides to address or structure its cyber risk discussions, and often, the extent to

which the business is dependent on IT for day-to-day operations will indicate its level of criticality to the business.

Based on industry data on scope and severity trends, along with the results of our survey, our view is that more education is needed at all levels within the enterprise. More than 80% of the directors we surveyed indicated that their company's IT budget includes funds for awareness and training. But often, cautions Bernard, the type of training is just as important as the budget or its scope."Static, computer-based training is insufficient to address the risk. Often, standard training programs are offered on a click-through basis, just like HR and compliance training," says Bernard. "The biggest vulnerability in most organizations is the people, and they can come in every day, and they can either improve the information security posture by being alert or not."

Still, there is room for optimism. With the right training, and with effective prioritization of potential threats, companies should begin to see some of the risk taper off in the future, according to EY's Tsantes. Even so, concerted effort across corporate America will be needed to turn the tide. "Cyber incidents should be smaller as time goes on," notes Tsantes. "An organization must amp up its detection capabilities to discover and shut down cyber incidents sooner over time." If you measure size and duration of impact regularly, the board could see trending, Tsantes adds.

Conclusion

There are several points that are key takeaways from the 2014 study around which this paper offers guidance and conclusions. First, most directors understand that business priorities and IT/cyber risk must be aligned for the company's cybersecurity program to operate effectively, although nearly half of respondents concede that such alignment is currently a challenge for them. Thus, better alignment between information security and key business priorities is a crucial process that many companies need to undertake.

Directors also acknowledge that they need more expertise among their ranks to effectively address cyber risk within the boardroom, and about two-thirds admit their composition needs to change to accomplish that objective.

Finally, requiring ongoing reporting and having an open dialogue with executive management about current weaknesses and vulnerabilities, as well as security threats and risk-appropriate responses, must be a part of the board's oversight process, but only about half of boards say they discuss cyber/IT risk regularly.

The bottom line is that in today's environment, no one defense will create an impenetrable barrier to cyber threats. Therefore, it is critical for the board and executive management to regularly evaluate—and reevaluate—which of the businesses' trophies are most valuable—and vulnerable—and thus require the lion's share of resources for protection. This, along with a concerted effort to elevate cyber risk to a strategic boardroom issue, will go a long way toward building a more effective cyber risk oversight program.

Figure 6

How often does your board discuss the following topics to oversee risk and enhance enterprise value?

	Regulary	Occasionally	Never
Cyber/IT security	54.85%	41.75%	3.4%
Emerging technologies	35.44%	54.37%	10.19%
Post-merger transaction integration	46.19%	36.55%	17.26%
Operational technology	53.40%	42.72%	3.88%
Compliance systems	71.84%	26.21%	1.94%
Social media	16.99%	65.63%	17.48%