Board Perspectives: Risk Oversight

Managing Cybersecurity Risk

Issue 44

In our knowledge-based economy where workers need round-the-clock access to relevant channels for communication, information sharing and collaboration, it is only natural that the use of web-based applications is becoming increasingly prevalent in the business environment. But from a security perspective, this trend has not been without cost.

In a recent survey, cyber threats and their potential to disrupt a company's core operations significantly was rated a top risk, with financial services and technology, media and communications companies rating it as a top five risk. Over the last two years, highly sophisticated cyberattacks across multiple industries that led to the loss of intellectual property and business intelligence have made the headlines.[1]

A recent report documenting the theft of intellectual property from more than a hundred U.S. companies by hackers backed by the Chinese military indicates that "phishing" emails and other tactics are being used to compromise organizations' security by exploiting human vulnerability and trust.[2]

A sobering thought: Despite the U.S. Security and Exchange Commission's requirements in the United States to disclose cyberattacks,[3] many believe the attacks reported are only the tip of a vast iceberg. One reason is that the overwhelming majority of companies are reluctant to talk publicly about the issue, for fear – which may be well-founded – of scaring away investors. A recently released study noted that 78.1 percent of more than 400 investors were "somewhat or very unlikely" to invest in a company with a history of being targeted in cyberattacks, while 68.7 percent were reluctant to invest in a company with a history of one or more data breaches.[4]

In this environment, and with so much at stake, organizations of all types must be more vigilant about protecting themselves from cyber threats.

Key Considerations

Over time, it is reasonable to expect investors to mature in their perspectives to recognize cyberattacks for what they are – a pervasive and often unavoidable issue. Cyberattacks are a growing problem not only for companies, but also for governments. Some of the largest and most high-performing organizations are experiencing literally thousands of network intrusion attempts by cyberattackers daily. What's needed is the

[1] *Executive Perspectives on Top Risks for 2013: Key Issues Being Discussed in the Boardroom and C-Suite*, research conducted by Protiviti Inc. and North Carolina State University's ERM Initiative, available at http://www.protiviti.com/toprisks.

[2] "Human Frailty Lets Cyber Thieves Attack, Expert Says," Brian Browdie, *American Banker*, March 19, 2013: http://www.americanbanker.com/issues/178_54/human-frailty-lets-cyber-thieves-attack-expert-says-1057669-1.html.

[3] See Protiviti's *SEC Flash Report, SEC Staff Provides Guidance on Public Companies' Disclosure Obligations Relating to Cybersecurity Risks and Cyber Incidents*, Oct. 2011: www.protiviti.com/en-US/Documents/Regulatory-Reports/SEC/SEC-Flash-Report-Cybersecurity-Incident-Guidance-101711-Protiviti.pdf.

[4] "Cyberattacks, Data Breaches Scare Off Investors, Study Says," John P. Mello, Jr., Network World, February 27, 2013: http://www.networkworld.com/news/2013/022613-cyberattacks-data-breaches-scare-off-267157.html.

capability to discover an incident fast, bring it to an immediate halt, and limit the damage.

It is also reasonable to expect cybercriminals, whatever their motivation, to use ever-more sophisticated means to gain control of online information and threaten critical infrastructure. Key security risks include potential leakage of sensitive information, unintentional upload of viruses to employee computers, and increased targeting of company employees for so-called social engineering attacks to gain information. Many organizations lack the process, technology and governance to combat this growing threat, including very sophisticated and stealthy advanced persistent threats (APTs), which can compromise multiple systems, collect mass data over time, and transmute such data to an attacker or attacker network.

There has been a dramatic increase in the number of companies that have experienced data breaches – many involving an APT – that did not have an effective incident response plan in place and therefore suffered the consequences. Now, a growing number of organizations want to improve their response processes. As discussed below, there are four key considerations.

Make incident response a top management priority. While preparation and the identification, containment and eradication of an incident are essential, one of the most important steps to building a response plan is gaining management support. Typically, unless the organization has experienced severe consequences from an incident, executives are reluctant to fund the development of a comprehensive incident response program. Even in cases where regulations or industry requirements mandate a program, organizations often succumb to common pitfalls such as:

- Developing a plan "good enough" to satisfy the business and non-information technology (IT) personnel in the organization.
- Failing to include an escalation plan, and appropriate roles, responsibilities and protocols for the plan's execution.
- Testing just enough to demonstrate compliance, but failing to test the plan thoroughly.
- Failing to enhance plans (e.g., not evolving procedures to address evolving threats, such as APTs).

Gaining executive sponsorship reduces the likelihood of these mistakes significantly.

Build a preventative human and technology security perimeter. Once the development of standards and practices is complete, companies must turn to employee education. The responsibility for security shifts from a technology-based focus to people who, through their actions and behaviors, have the most significant role in securing the enterprise. By building a strong communication program and heightening the overall risk consciousness, organizations can help their employees recognize risky behavior and respond to attacks, thus creating a "human security perimeter."

Employee education and awareness, alongside strong technical security controls such as antivirus, antispyware and web-filtering technology, will help clarify for the appropriate personnel how to use the technology to achieve the expected results, while also reducing the likelihood that these risks will impact the business.

Use escalation protocols to increase visibility at the top. We're still too often seeing compromised companies handling security breaches only at the IT level, with the board and/or executive management viewing these matters as just another "IT issue." Criteria should be established for an incident response program within the context of the company's regulatory, legal and business objectives. To this end, there should be a clear definition of the "events" that rise to the level of an incident using parameters such as monetary, earnings, systems, and B2B or B2C impact. More importantly, the notification requirements to escalate an event to the board when an event is declared should be defined.

Create an operational framework for incident response. Companies should establish an incident response program that has management visibility and sponsorship. Based on an understanding of (1) the company's regulatory, legal and contractual obligations; (2) privacy requirements; (3) the notification policy related to a cybersecurity incident; and (4) the complexity of international operations, an incident response plan should establish the operational framework for the incident response team. For example, the plan should:

- Integrate and complement existing information security programs and ensure technology has up-to-date and complete network documentation of all internal and external connections to/from the firm.
- Include input from appropriate stakeholders of the incident response team – compliance, IT, security operations, corporate security, corporate communications, regulatory and legal affairs, and appropriate line of business representatives.
- Clearly assign roles, responsibilities and accountability within the organization.
- Include escalation protocols, paths and communication procedures to ensure appropriate stakeholders are involved in key decisions pertaining to response to and disclosure of specific incidents.
- Address regulatory obligations regarding incident response or breach disclosure.
- Ensure trusted and qualified parties are available should the scope or specifics of an incident exceed the resource availability or capabilities of in-house personnel.
- Ensure appropriate parties maintain key contacts in law enforcement and the media to expedite actions as dictated by the organization.
- Require periodic testing of the incident response program.

While not an all-inclusive list, the above illustrative points help to increase the incident response plan's effectiveness. The organization also should consider retaining appropriate external expertise (including on a global basis, if operations are international) and carefully consider involvement of government agencies. If a security incident occurs, the plan should consider the potential duty to preserve relevant information and evidence; any potential legal and regulatory actions; and the cost, time and burden associated with e-discovery.

Questions for Boards

Following are suggested questions that boards of directors may want to consider, in the context of the nature of the entity's risks inherent in its operations:

- Are effective incident response processes in place to reduce the occurrence, proliferation and impact of a security breach? Do key stakeholders support the development of a plan appropriate to the organization's scale, culture, regulatory obligations and business objectives?
- Is the company's incident response plan complemented by procedures that provide instructions regarding actions that should be taken in response to specific types of incidents? Are these procedures evaluated periodically?
- Is it clear which events would require the board to play a key role in response efforts, as opposed to just receiving an update after the fact or during the postmortem?

How Protiviti Can Help

Our experience and dedication to the development and enhancement of world-class incident response and forensic investigation practices related to security incidents and intrusions have resulted in deep expertise in response execution, forensic analysis and response plan development. We assist companies around the world in preventing cyberattacks on their IT environment and overall enterprise as well as provide incident response and forensics investigation services in an effort to reduce the impact of an attack while providing support to recover from it. We have worked with companies in this space to address their corporate governance, employee communication challenges, and escalation processes. In addition to being one of only eight firms in the United States approved by the PCI Council and a major credit card brand to provide incident response and forensic investigation services, Protiviti was engaged to provide response services to two of *CSO Magazine*'s "Top 15 Worst Rated Security Breaches of the 21st Century."

About Protiviti

Protiviti **(www.protiviti.com)** is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is partnering with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on www.directorship.com/author/jim-deloach/ in the "Blogs & Opinion" section. A compilation of blog posts and articles is maintained and categorized by author's name. Twice per year, the previous six issues of *Board Perspectives: Risk Oversight* will be consolidated into a printed booklet that will be co-branded with NACD. Protiviti will also post these articles at Protiviti.com.