Board Perspectives: Risk Oversight

Managing Cyber Threats with Confidence

Issue 66

Cybersecurity attacks continue to be the focus of front-page media coverage and remain a highly relevant topic in the boardroom. Cutting across strategy, risk management, change management and access control, information security is concerned with confidentiality, integrity and availability of information systems. Below, we address this important issue.

The realities of risk management are that risks are impossible to eliminate, resources are finite, and risk profiles are ever-changing. Such is the case with cyber threats. That is why it is important to focus on protecting an organization's most important information assets and systems (the "crown jewels") by understanding the changing threat landscape and risk tolerances and preparing for the inevitable incidents.

Key Considerations

Few businesses have given focused attention to defining their information asset crown jewels across the enterprise or thoroughly assessing their tolerance for cybersecurity risk. In reality, most think their risk tolerance is low, but act as though it is relatively high. Unknowingly, they apply the same high-risk tolerance to *all* systems and information assets. In effect, few focus on the information assets and systems that really matter.

Getting close to secure is elusive. How many organizations can manage all cybersecurity risks effectively? How many can prevent a well-orchestrated attack by an IT contractor hired to operate within perimeter defenses? There aren't many. However, with targeted investments and tolerance for higher levels of security, organizations can get much closer to securing their crown jewels.

Everyone recognizes security risks in their homes. Most homeowners take basic measures – such as locking all entrances, leaving lights on when they're out, or installing affordable security systems – to reduce the risk that they will become a target for criminals. Others go even further with their efforts to stay secure, such as choosing to live in a gated community. But does anyone really believe any or a combination of these measures are guaranteed to prevent a determined attacker who targets a residence? Probably not.

Most households accept the risk. In addition to making their properties difficult to break into, they take out homeowners insurance on contents and valuables to cover residual risk. Many may rationalize their focus on the few things that really matter to them, such as valuable heirlooms and important documents and records, and take additional precautions. While most do not accept the idea of their homes being burglarized, they are willing to go only so far to inconvenience themselves and/or spend money to protect their property.

Businesses are not very good at applying this rational thought process and have a false sense about how secure they can be on an enterprisewide basis. Security is not just about hacking and technical breaches. Most cyberattacks, while clever, are not necessarily technical. They may draw on hacking techniques, but often this skill is not needed, as an attacker only needs to be hired as a contractor to get beyond the perimeter. And even this penetration might not be necessary, as it is not difficult to get past security in most organizations.

Rather than attempt to cover the waterfront, we've chosen to discuss three key points to achieving the appropriate focus on IT security:

Focus on what is most important to protect the crown jewels – The IT security focus of many organizations tends to be somewhat generic rather than targeted, resulting in all-systems-are-equal protection measures, lack of sufficient attention to the most vital assets, and unnecessary costs. Identification of high-value data, information and information systems requires the collaboration of the IT organization and business leaders to agree on the organization's tolerance for risk relative to different assets; this helps IT security management focus on protecting the most critical areas. Under the oversight of the board of directors, they should consider questions such as:

- What are the organization's most critical data, information assets and information systems (crown jewels)? Why are they of highest value? What can we not afford to lose?
- Where do the crown jewels reside? Are we certain they only reside in those places?
- How are they accessed – and through how many systems?
- Who is authorized to access them? Are they accessible through IT support contractors? Who authorizes these contractors and on what basis?

These and other questions help to focus the organization's preventive and detective security measures and incident response plans.

Understand the changing threat landscape – In a recent global survey, cyber threats and their potential to disrupt a company's core operations were rated as a top risk, with almost all industry groups rating them as a top five risk. In addition, privacy/identity and information security issues were a top 10 risk.[1]

Do directors understand these risks as well as the other top risks their companies face? Not likely. That is why reports of cyberattacks of unprecedented scale across multiple industries, resulting in the loss of intellectual property, business intelligence and reputation, have sounded alarms in boardrooms. Directors are starting to recognize that cybersecurity is an enterprise security issue, not just an IT security issue.

Key security risks include potential leakage of sensitive information, unintentional upload of viruses to employee computers, and increased targeting of company employees through so-called social engineering to obtain confidential information. Many organizations lack the processes, technology and governance to combat today's sophisticated cyber threats effectively, including advanced persistent threats that can compromise multiple systems, collect mass data over time, and transmit such data to an adversary or attacker network.

Based on the company's crown jewels, the nature of its industry and operations, and its visibility as a potential target, management should assess the organization's cybersecurity risk and ask:

- Who are our likely adversaries?
- How are they likely to attack us?
- Where are our biggest vulnerabilities?
- What is our exposure to contractors and insiders?
- How effective are our current internal controls in managing these issues, and what are they costing us?
- Do we conduct penetration testing? If so, what are the results?
- What issues are raised by internal and external auditors?
- What has been the nature and severity of prior cyberattacks? How will we know if we've been attacked again?

[1] *Executive Perspectives on Top Risks for 2015: 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 www.protiviti.com/TopRisks.

- Do we have a clear understanding of the impact to the business if anything occurs?

Answers to these and other questions can help to clarify the changing threat landscape and provide direction to the implementation of security measures.

Prepare for an incident/crisis – Despite the precautions organizations may take, cyber incidents of varying magnitude are inevitable. That is why companies need to be proactive about developing an effective incident response plan. Much more than a mere best practice, a response plan is also an obligation and demonstration of due diligence, especially for an organization that maintains sensitive data or personally identifiable information (PII).

In the past, many organizations conducted annual or semiannual business continuity tests. These tests were full simulations of how a business would respond to a relatively *low*-likelihood incident. Now that organizations face the specter of a relatively *high*-likelihood business continuity incident, it is ironic that very few organizations prepare properly and even fewer perform continuity tests. It is essential to apply the same logic of testing a business continuity program to an effective incident response program. Being proactive enables organizations to address the unexpected – and plan for the worst.

Effective incident response processes are critical to a company's preparedness to reduce the impact of a cyberattack. Executive sponsorship is needed to ensure a comprehensive incident response program is funded. Traditionally, few executive stakeholders outside of the chief information officer's organization have been engaged in the implementation of an incident response plan. However, with the emergence of the National Institute of Standards and Technology's (NIST) cybersecurity framework, breach disclosure requirements, and industry regulations and standards dealing with PII, senior executives are now more apt to support these initiatives, particularly given recent media coverage of significant breaches. These programs should integrate and complement existing IT security; incorporate the perspective and participation of various stakeholders (e.g., compliance, IT, security operations, corporate security, corporate communications, regulatory and legal affairs); and provide clear direction and core processes that are followed in the event of an incident.

The program also should assign roles, responsibilities and accountability to groups and individuals within the organization, include escalation paths and communication procedures to ensure appropriate stakeholders are involved in key decisions pertaining to response and disclosure, and provide instructions regarding actions to take in response to specific types of incidents. For example, the method of responding to a distributed denial of service (DDoS) attack varies greatly from the method of managing a malware incident.

Incident response plans must be evaluated on at least an annual basis and address regulatory obligations regarding incident response or breach disclosure. It must ensure appropriate parties maintain key contacts in law enforcement and the media to expedite actions as dictated by the organization. Also, it should ensure that trusted and qualified parties are available in the event that the scope or specifics of an incident exceed the resource availability or capabilities of company personnel.

Questions for Boards

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

- Have we identified our most critical assets that we simply cannot afford to lose and/or systems to which unplanned outages cannot be tolerated at any cost (the so-called crown jewels)? Do we know whether and how they're being protected? Does our security strategy differentiate our crown jewels from general cybersecurity?
- Do we assess periodically our threat landscape and tolerance for risk related to our crown jewels? Do we actually believe our most critical assets and systems are secure and/or the risk events we have identified cannot happen?

- Are our strategies for reducing the risk of security incidents to an acceptable level proportionate and targeted? Are we being proactive and periodically testing our incident response plan to determine its effectiveness?
- Do we understand which security incidents cannot, and will not, be tolerated? Are effective incident response processes in place to reduce the risk of a security breach occurring, proliferating or having a significant impact? 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 to take in response to specific types of incidents? Is the plan evaluated periodically? Is it clear which events require the board to play a key role in overseeing response efforts?

How Protiviti Can Help

We provide a wide variety of security and privacy assessment, architecture, transformation and management services to help organizations identify and address security and privacy exposures (e.g., loss of customer data, loss of revenue, or reputation impairment to a customer) before they become problems. We have a demonstrated track record of helping companies react to security incidents, establish proactive security programs, deal with identity and access management, and handle industry-specific data security and privacy issues. Our experience and dedication to the development and enhancement of world-class incident response and forensic investigation practices have resulted in deep expertise in security strategies, response execution, forensic analysis and response plan development.

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, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. 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.nacdonline.org/Magazine/author.cfm?ItemNumber=9721. Twice per year, the six most recent 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.**

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®
Risk & Business Consulting.
Internal Audit.