Cybersecurity: What Are the Boardroom Implications?

By Dan Swanson, KnowledgeLeader contributing writer

Safeguarding assets has been an important objective of all organizations for centuries. In today’s digital age, however, what does safeguarding your assets really mean? Who is responsible for it? And how is “protection” actually achieved? As important, what threats, risks and challenges does cybersecurity add to the organization’s already mounting responsibilities?

“Although the risks presented by technology are not new to the corporate arena, the dynamic nature of cybersecurity presents a unique challenge to companies and boards. The increasingly fast pace of technological changes creates many targets and makes defense systems more complex and more difficult to manage and control,” as noted in CyberSecurity: Boardroom Implications, a 2014 National Association of Corporate Directors (NACD) paper.

WHO IS RESPONSIBLE FOR INFORMATION ASSET PROTECTION?

While chief information security officers and chief financial officers are important players regarding information asset protection and security, they are not the true “guardians” of the organization’s critical informational assets. For example, in hospitals, CFOs are not responsible for safeguarding patient records; at insurance companies, they are not the guardians of policyholder records. In the pharmaceutical or technology sectors, the company’s crown jewels (its intellectual property) are not the direct responsibility of the CFO or the CISO.

All of these forms of data have associated expenses and are used to generate revenues (billings, annual fees, royalties), for which the CISO has ultimate security oversight. The CISO in turn must ensure the integrity of the chain of custody by enforcing rules applicable to key managers and other authorized personnel in their roles as the day-to-day “guardians.” In short, internal control is affected by people at every level of an organization. In fact, many managers are more directly responsible for day-to-day asset protection than the CISO or CFO.

WHAT ARE SOME IMPLICATIONS?

Addressing the following questions will help determine how to protect your digital assets, ensure cybersecurity is appropriately considered, and let you know what actions to take.

- Will an organization’s information security management system become critical to the safeguarding of the CFO’s financial records? Will those systems emerge as the main means of safeguarding an organization’s assets?
- Will CFOs and finance staff need to understand and implement informational asset protection measures to be effective in their roles of supporting the guardians of the organization’s assets?
- Will we need more guidance on the definition, classification and protection of information assets?
- Will CISOs need to work more closely with and educate the finance function (and all operating departments, really) about how to best implement a sustainable information protection and security program?
- Should the organization establish a data management function and data governance policy, standards and procedures? Both the function and governance could be headed by a senior...
manager reporting to the chief operating officer or chief executive officer. What role(s) should the chief information officer take in information protection?

• Will the board and CEO need to provide more in the way of expectations?
• Will internal audit and external audit spend more resources on evaluating the protection of all of an organization’s assets, both physical and digital? The internal audit function in particular needs to think more strategically about enterprise-wide security and ensure that enterprise-wide risk management is a guiding theme for prioritizing the organization’s efforts.

The bottom-line: Top management must implement an information security management program that truly safeguards all assets of the organization and also addresses the many risks, threats and challenges involved with cybersecurity.

Cyber-Risk Oversight Handbook, a NACD publication, in collaboration with American International Group (AIG) and the Internet Security Alliance, takes the position that directors should ask questions. The publication presents five key principles to consider:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risks as they relate to their company’s specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber risk management should be given regular and adequate time on the board meeting agenda.
4. Directors should set the expectation that management will establish an enterprise-wide cyber risk management framework with adequate staffing and budget.
5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate or transfer through insurance, as well as specific plans associated with each approach.

Are all your organization’s assets appropriately protected in the digital age? I recommend making this a regular topic of discussion at your management committee meetings, and also put it on the board agenda on a regular basis. An effective tone at the top starts with top management and the board taking action to implement appropriate security controls.

The board should ensure it has sufficient information and expertise to ask the right questions of management at regularly scheduled board meetings. They should demand both internal audit and risk management assistance in assessing cyber risk and the adequacy of management’s programs for managing it. The CEO should ensure the executive management team provides appropriate and ongoing attention to this critically important subject.

Good luck making a difference.

KnowledgeLeader is a subscription-based website that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals save time, manage risk and add value. Free 30-day trials are available.

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 Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

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