The IBIT Report
A Publication of the Institute for Business and Information Technology

Richard Y. Flanagan, Ph.D.
Director of IT Audit & Cybersecurity Programs
Fox School of Business, Temple University

Janet L. Yeomans
Director/Trustee, Delaware Family of Funds
Director, Okabena Company

Implementing Board Oversight of Cybersecurity

ADVICE FOR BOARDS JUST STARTING OUT

Fox School of Business
TEMPLE UNIVERSITY®

The IBIT Report

Wyndetryst Print & Web Design
Art Direction, Layout, Editing | wyndetryst.com

 ISSN 1938-1271.

The IBIT Report is a publication for the members of the Fox School's Institute for Business and Information Technology. IBIT reports are written for industry to provide actionable knowledge and are based on rigorous academic research and vendor neutral analysis. Each report focuses on an important cutting edge topic that is of interest to our members.

For additional reports, please visit our website at **http://ibit.temple.edu.**

Disclaimer: The conclusions and statements of this report are solely the work of the authors. They do not represent the opinion of Temple University or the members of the Fox School's Institute for Business and Informational Technology (IBIT).

Review process: IBIT reports are sourced, reviewed, and produced as follows. The managing editor oversees this process. The editor and editor-in-chief consult on topics and identify new sources of reports. The editor typically works with authors who are interested in writing reports and provides feedback on initial drafts. Completed reports are first screened by the editor-in-chief. After approval the report is sent out for review to two members of the editorial board. The editor-in-chief assesses the completed reviews and provides further guidance to authors. Final reports are then professionally produced and made available to IBIT members.

Foreword

Many well-known companies, such as Verizon, Target, and Home Depot, among others, received an enormous amount of undesirable publicity following data breaches that resulted in millions of dollars in losses.

While oversight of cybersecurity risk management should be a regular agenda item for boards of directors, many boards do not have the knowledge or experience to address it. This IBIT Report is a call to action for boards, urging them to think more carefully about their investment of time and attention in securing their information assets. For boards just starting out as well as those already attempting to deal with this issue, the authors detail the steps to define roles and responsibilities, influence corporate culture, develop processes, and establish partnerships. This advice can serve as a guide for those boards of directors interested in protecting their companies from future breaches.

Bruce Fadem
Co-Editor-in-Chief
March 2016

David Schuff
Co-Editor-in-Chief
March 2016

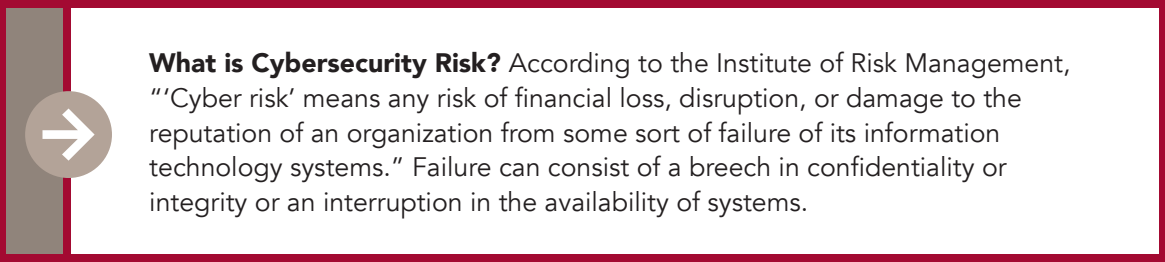
Introduction

Many well-known and well-respected companies, when hit by hackers, have had their customers' data security compromised along with their reputations. Others have not. Why?

A key differentiating factor at play is the role that boards, executives, and security personnel can have in creating a security culture that makes them more resistant to the negative impacts of breaches. In truth, the question is not if a cyber incident will happen, but rather when and how effectively the company will detect it and respond. The corporate executives, IT technical experts, and the board should work in partnership to ensure their organization is prepared to effectively handle such events when they do occur.

Therefore, we invite you, as a board member, to use this report as a manual for how to take action around cybersecurity risk quickly and decisively and protect your hard-won reputation and your company for the long term. Only by taking steps now can you **help prevent potentially devastating future consequences.**

The report has been broken down into easy-to-navigate thought modules, where you tackle issues related to cybersecurity one-by-one. If you have questions about how to make cybersecurity a real priority in your C-suite, please do not hesitate to contact the authors at **janyeomans@me.com** or **Richard.Flanagan@Temple.edu.**



What is Cybersecurity Risk? According to the Institute of Risk Management, "'Cyber risk' means any risk of financial loss, disruption, or damage to the reputation of an organization from some sort of failure of its information technology systems." Failure can consist of a breech in confidentiality or integrity or an interruption in the availability of systems.

Executive Summary

Given the massive potential costs to a company's bottom line and reputation due to a data security breach, cybersecurity risk has become a permanent aspect of business risk that must be actively managed and integrated with business decision-making and processes. Oversight of cybersecurity risk management is now an integral component of good governance and must be a regular agenda item for boards of directors. To effectively protect the corporation from consequences of a loss of information assets, management and directors must build a constructive partnership. This report is primarily directed to boards and corporate managements who are aware of the need to address cybersecurity risk but do not yet have a robust process in place.

THE THREE CONDITIONS

To build such a partnership, **three conditions** must be met:

1. It is necessary to identify a clear management "owner" of cybersecurity risk who has a close working relationship with the CEO.
2. The board must decide where in its structure primary oversight responsibility will lie.
3. Finally, the designated cybersecurity owner must communicate with the assigned directors using business risk language the board understands.

THE THREE MEETINGS

We suggest **three meetings** as the foundation for such an evolving partnership:

1. A security briefing to ascertain if the security team has accurately identified the key business risks posed by a cyber incident.
2. An assessment of the company's security environment, including the results of a vulnerability analysis and management's responses to findings.
3. A review of management's incident handling processes and the status of their preparedness, including clear identification of roles and responsibilities.

Critical elements include:

- Existence of a standing crisis management team
- Clear process for escalating incidents as they emerge as more serious threats
- Process for contacting regulators promptly
- Readiness of top-drawer statements and process for handling media inquiries

By working together, management and the board can build a robust process for protecting the interests of owners, customers, employees, and suppliers from risks to the business posed by loss of information assets.

The Need for Board Involvement with Cybersecurity

The growing list of reported breaches and their impacts make a compelling case that cybersecurity risk is a permanent aspect of business risk that must be factored into business decisions and operations at the company level and into the responsibilities of directors as a component of good governance. Indeed, the numbers are scary.

Verizon's 2015 Data Breach Investigations Report discusses more than **79,000** security incidents with **2,122** confirmed breaches in **61 countries**, including JP Morgan, MasterCard, Visa, Subway, Goodwill Industries, Uber, Trump Hotel Collection, Adobe Systems, and others.

Documented losses for some recent breaches include **Target** (2013): **$162 million** to date with several law suits still outstanding. **Home Depot** (2014) estimates its costs at **$63 million** but says it is too soon to really know.

Major Company Losses

VERIZON

Verizon's 2015 Data Breach Investigations Report

79,000
security incidents

2,122
confirmed breaches

61 countries

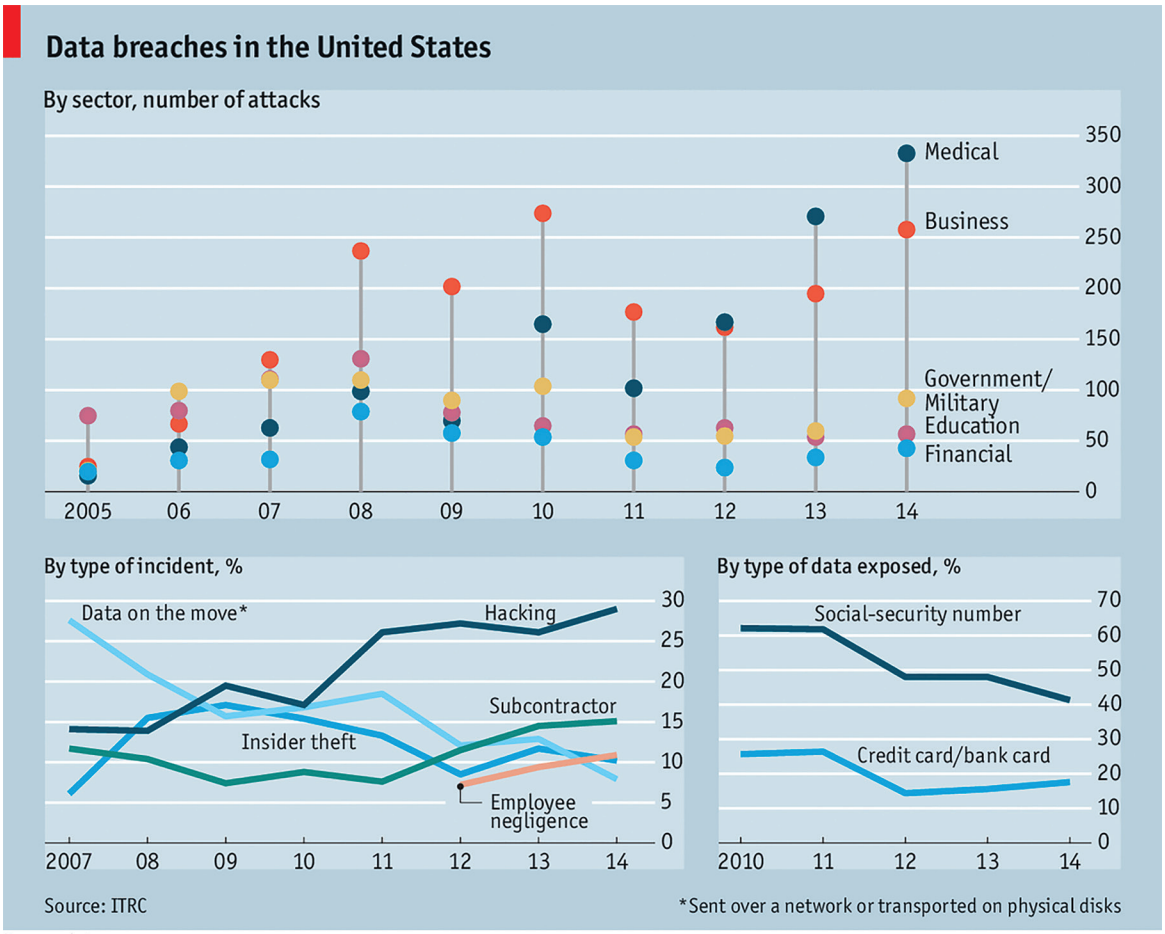
TARGET

$162 million
in losses

HOME DEPOT

$63 million
in losses

A recent Economist article documents the growing problem:



Economist.com

While statistics and losses such as these demand that cybersecurity be a high priority for every corporation and board of directors, recent data indicate that this is not yet the case. As recently as 2014, **SEC Commissioner Luis A. Aguilar** spoke to the New York Stock Exchange on the topic of "Cyber Risks and the Board Room." His central message was:

> *"…evidence suggests that there may be a gap that exists between the magnitude of the exposure presented by cyber risks and the steps, or lack thereof, that many corporate boards have taken to address these risks."*

Mr. Aguilar suggests that boards need to provide **meaningful oversight** of the company's proactive actions to mitigate these risks.

Cybersecurity:

Navigating Unfamiliar Territory

A possible explanation for the apparent lack of focus is that many senior executives and boards find themselves in unfamiliar territory when it comes to formulating policies and oversight processes that address cybersecurity risk.

Few among them have backgrounds in information technology, let alone cybersecurity. Jean-Louis Bravard notes that in looking at the boards of U.K. banks he found only one director with technical experience. When ISACA asked, "How involved was the board during the last fiscal year in regard to specific action or request on cybersecurity preparedness?," only **14%** responded that they were actively involved (see the responses in the chart below). However, in the same survey, **58%** of respondents said they should be actively involved in cybersecurity matters.

Respondent Involvement

Actively Involved	**267**
Moderately Involved	**662**
Minimally Involved	**686**
Not Sure of Involvement	**283**
Not Answered	**37**
VALID RESPONSES	**1,898**
TOTAL RESPONSES	**1,935**

How to Build An Effective Cybersecurity Partnership

With the need clear, how might a company and its board go about building an effective partnership to manage cybersecurity risk? Importantly, the risk must be recognized as dynamic in nature.

Unlike the risk of fire at a specific factory or an earthquake at a particular corporate building, the very nature and potential magnitude of cybersecurity risk **changes in real time**.

With this understanding, the first step should be to **clearly define roles and responsibilities.**

Roles & Responsibilities

OWNERSHIP OF CYBERSECURITY RISK

In order to determine proper roles and responsibilities surrounding cybersecurity in your corporation, you should ask yourself the following questions:

- Within the corporation, who "owns" cybersecurity risk?
- Where are the skills and responsibility within the corporate structure?
- Is the owner a member of the CEO's inner circle of advisors?

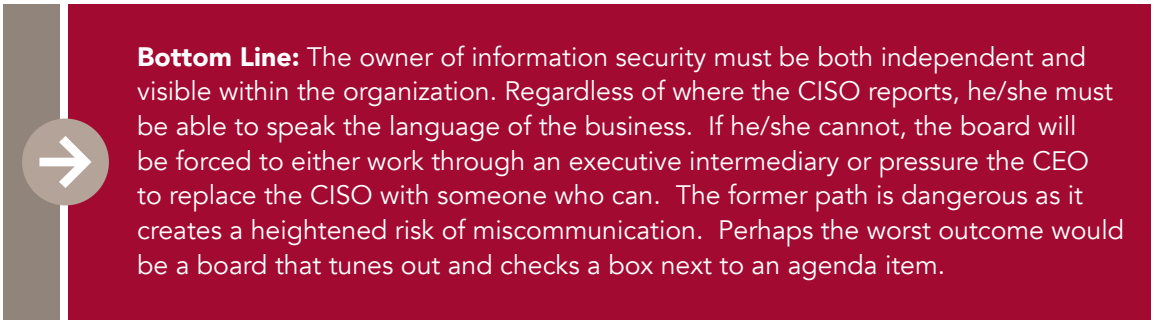
These questions are important because potential risks need to be factored into every business decision and the CEO must clearly demonstrate that doing so is integral to business conduct.

CYBERSECURITY MANAGEMENT WITHIN THE BOARD

At the board, will cybersecurity risk be delegated to a standing committee of the board or owned by the board as a whole? If the former, the full board must be regularly apprised of the committee's activities. Either way, each board member must be comfortable that, should a cybersecurity incident occur at the company and legal action ensue, he/she would be confident being deposed on board oversight of cybersecurity risk.

If the board's decision is to delegate oversight of cyber risk to a committee, the likely alternatives are the **enterprise risk committee**, if there is one, or the **audit committee**. Although an enterprise risk committee is a natural home for cybersecurity risks, such committees exist in only half of the boards in the U.S. While cybersecurity is well within the audit committee's purview, it is important that it be viewed as a unique issue, not a variation of a related but distinct issue, such as compliance or business continuity. Another consideration is that audit committees are assuming ever more responsibilities with the proliferation of regulations and financial reporting requirements. As a result, their meeting agendas are packed. Having time for discussion and questions is imperative, so an audit committee charged with cybersecurity oversight will likely need to **extend its meeting times**.

Once the board has assigned oversight responsibility within its own ranks, the next step is to clearly identify who on the management team owns responsibility. Is there a Chief Information Security Officer (CISO)? If so, to whom does he/she report: **the CRO, the CFO, the CIO**? There is a clear segregation of duties conflict if the CISO reports to the CIO. The CISO needs to point out problems with how IT is operating and, if not independent, this might prove impossible. Similarly, a CFO or CRO might see information security as a subset of his/her financial compliance requirements. This is often cited as a commonly made mistake.



Bottom Line: The owner of information security must be both independent and visible within the organization. Regardless of where the CISO reports, he/she must be able to speak the language of the business. If he/she cannot, the board will be forced to either work through an executive intermediary or pressure the CEO to replace the CISO with someone who can. The former path is dangerous as it creates a heightened risk of miscommunication. Perhaps the worst outcome would be a board that tunes out and checks a box next to an agenda item.

Implementing a Cybersecurity Risk Process

Within the corporation, the first step in establishing a cybersecurity risk management process is to understand that cybersecurity is a business risk, not a technical IT or compliance issue.

Cyber issues must be framed in business risk terms. Here are some questions to consider as you **formulate an understanding of cybersecurity risk** that is integrated into your larger framework for business risks:

- Which information assets are most valuable, where do they reside, and who is authorized to access them?
- What are the worst-case losses if business processes allow unauthorized access to those assets?
- How can the risks be mitigated by lessening their likelihood or impact?
- Can the risk be reasonably transferred? If so, at what cost?
- Are there risks that can be eliminated by improving business processes?

Business leaders and process owners must be held accountable for ensuring continuous attention to making cybersecurity an integral aspect of their operations, and metrics of success must be components of business reviews alongside traditional financial metrics. The tone must indeed be set and maintained at the top and woven into the fabric of corporate culture. For its part, the board must **hold company executives accountable** for successfully protecting key information assets on par with other key business deliverables.

First Action Steps of the Partnership

Having laid the groundwork with roles and responsibilities and corporate culture, we are now ready to build the partnership between corporate management and the board to effectively oversee cybersecurity risk. We propose that whichever committee the board assigns this role to (here after: "the Committee") should plan **three separate meetings** with the CISO, the Internal Auditor, and, preferably, an external security expert.

Meeting One
Security Briefing

Its goal is to explore what business assets are at risk, who the attackers are likely to be, their tactics, and what the organization is doing to mitigate potential losses.

Meeting Two
Security Culture Audit Review

The focus of this session should be on the tone of the business' security environment. For instance, are security considerations thoroughly integrated into all business processes?

Meeting Three
Incident Response Meeting

This meeting answers questions regarding whether a company has a process at the ready in case a major security incident does occur as well as who will do what and when.

Let's consider the agenda for each of these three meetings in more detail.

Meeting One
The Security Briefing

Meeting One Overview

At its first meeting on cybersecurity, the Committee should request a briefing by the senior security professional on:

- What does management see as the 3-5 most serious business risks stemming from IT facing the company?
- What types of losses the company could face?
- What specific actions have been taken in reference to these specific risks?

Such a meeting will give members of the Committee insights into the organization's security structure as well as the alignment of the corporation around cyber risk management as a business priority. There is a **series of questions** the committee should ask regarding who will present this information.

Questions Regarding Who Will Present Information at Meeting One

- ☐ Is the CISO presenting or is one of the executives?
- ☐ If an executive is chosen to present the information, the Committee should wonder why security can't speak for itself. Does it exist?
- ☐ Is it adequately staffed by people with strong skills and experience?
- ☐ How is it positioned in the organization?
- ☐ Is the security lead too technical?
- ☐ Likewise, if the CISO is presenting, does that person speak and understand the business' language?

NOTE: *A security leader needs to be able to speak to the technology issues but also business risks and potential impacts.*

STEP 1: Determining Top Business Risks

Two often heard security truisms are **"No one is ever 100% secure"** and **"No one can afford to secure everything."** These statements, taken together, point to one of the key areas in which the Committee can significantly help the organization's cybersecurity effort.

- Since no company can afford to secure everything, which information assets are going to get attention and resources?
- What are the decision criteria for distributing the budget in terms of manpower and dollars?
- Are these criteria resulting in the right choices?
- What are the trade-offs in terms of risk reduction and higher expense?

These are business decisions, not technical decisions, and **the Committee must be comfortable** with the process by which management makes them.

The Committee must further exercise its judgment as to whether or not the identified risks conform to board members' understanding of the business by answering the following questions:

Questions Regarding Risks

- ☐ Are the risks specific to the company or are they a generic list of cyber risks?
- ☐ Are the risks linked to business losses in a logical, direct manner?
- ☐ Are there other information based business risks that board members think might be more serious?

STEP 2: Determining Potential Losses

The security team should have a clear focus on the most significant losses facing the business from a cyber attack. The discussion must be informed by data and robust analysis and not merely conducted at a conceptual or anecdotal level. In determining what the corporation's most important information assets are and the potential losses associated with them, the Committee needs to think of two different types of information assets: **data and systems.**

Deciding which data could trigger the greatest loss is not straightforward. Data losses can have long-term consequences up to and including viability of the company as a result of financial costs of remediation, loss of customers and reputation, and legal liability. For example, the loss of key intellectual property could threaten the organization's value proposition similar to Sony's loss of control of its movies and games. Loss of credit card data has caused customers to become wary of Target, Home Depot, and other retailers. Finally, the loss of sensitive data might jeopardize the organization's ability to run its business, as happened to Global Payments when it was suspended from the list of PCI compliant payment companies because of a breach.

Briefings must cover information on the company's data and its systems, as compromises to either can have serious financial and reputational consequences. For instance, a Distributed Denial of Service (DDOS) attack, which makes a company's systems sluggish or unavailable, as suffered by the U.S. banking industry, can cause loss of revenue and damage a firm's reputation. A recent U.K. survey estimated that DDOS attacks could cost 40% of U.K. companies 100,000 GBP/hour (approximately $155,000/hour) at peak time. Another type of attack, called ransomware, encrypts all of a company's data using programs, such as Cryptolocker, followed by a ransom demanded for its release. Joseph Bonavolonta, an assistant special agent with the FBI, said, "To be honest, we often advise people just to pay the ransom" because efforts by the Bureau to defeat the encryption used have proved futile. How much would a day of no IT-enabled business processes be worth?

STEP 3: Identifying Action Steps

The final part of this briefing should focus on the steps security has taken to address the identified risks. Every company of any size has a security team that has implemented some basic security measures. The likes of role-based security, employee education, perimeter defense (firewalls, IDS/IPS, etc.), and malware protections are baseline security measures that every company should have in place.

Summary: Such a briefing is a good place to start for any Committee that is in the beginning stages of integrating cybersecurity risk into its governance practice. It will give members an understanding as to whether or not the company's security efforts are in good hands. If in doubt, then the Committee and executive management need to explore how to get the proper leadership and resources (money and personnel) assigned to their security initiative. If things went well, the Committee can move on to our next two selected topics. Such cybersecurity briefings should be a standing item on the Committee agenda. While each board will have different needs, most will likely want a dashboard to track changes in risk assessment quarterly with in-depth reviews annually. If a breach has occurred at the company or a competitor, then monitoring and review will be more frequent. Importantly, these briefings will also demonstrate to the company that the board is actively engaged in understanding this set of business risks and that it takes its governance responsibilities in this area very seriously.

Meeting Two

Assessing the Company's Security Environment

Compliance vs. Security

Security controls and compliance are often conflated. They are in fact fundamentally different.

COMPLIANCE		SECURITY
Compliance and financial controls monitor black-or-white adherence to defined rules and standards. They therefore cannot identify or assess risks beyond the purview of the compliance requirements, which are typically employed to prevent a recurrence of something detrimental that has happened in the past.	VS	Security controls are necessarily dynamic and proactive, as they identify likely intruders in real time and keep them out to the extent possible or detect failure and kick the intruders out immediately. Security controls operate in space that is continuously changing and therefore consistent vigilance is required.

Having noted that **security and compliance are not the same**, it is important to recognize that in some circumstances **they are complementary**. Regulatory (e.g. SOX) or industry compliance (e.g. PSI) provides an awareness of some security issues and ways to address them. However, while regulations tend to be reactive and based on history, security must be grounded in the present and forward looking. When allocating corporate resources, care must be taken that compliance, a more established corporate function, does not draw much needed resources away from security without helping. There needs to be a good working relationship between the two functions. In a recent Gartner post, **Anton Chuvakin** raised this very point forcefully:

> *"… many environments buy security tools for compliance and then do not use them at all [not even for compliance], or only use them to the extent needed to satisfy the most creatively minimalistic interpretation of a particular mandate or regulation."*

A company that conflates compliance and security is at significant risk, as is a company where compliance and security exist separately and function independently. Employee training and behavior driven by senior management expectations and actions are critical and contribute to a company's culture surrounding cybersecurity. The Committee should ensure that management is **investing in effective** training about security risks and potential consequences of an incident while setting a high standard for accountability by example of its senior leaders.

For example, every employee should understand the importance of:

Cybersecurity as Part of the Company Culture

As with compliance, security is rooted in an organization's culture. When well done, its importance is a tone set at the top and understood throughout the company. It's a discipline that the entire organization must respect and follow for it to be effective. While action steps for creating this culture will differ in specifics from company to company, in general the CEO and senior management will include cybersecurity in discussions of business decisions and in reviews of business results. In addition, management will set expectations at a high level through policies and standards and will talk about cyber preparedness in employee group meetings. Management will also demonstrably "walk the talk" by completing training courses and practicing all company housekeeping safeguards. Employees must be educated about risks to the enterprise and controls to mitigate those risks. Employees at every level must be held accountable for upholding corporate standards, and consequences for failing to do so must be visible. Auditors will test the internal control environment for weaknesses.

Housekeeping

In an article on the seven largest losses of 18.7 million medical records, only two of the incidents were hacks in which outside criminals obtained records by breaking into the organization's systems. The rest, 71%, resulted from lost or stolen physical media. Lost PCs with inappropriately copied data and drives stolen from data centers are lapses in good security housekeeping, not the work of nefarious cyber criminals.

Employee Behavior

Phishing attacks work because people, unaware of the risk, do not behave appropriately. Verizon estimates that the average time from the first email of a phishing campaign to the first "successful" click-through is one minute and twenty-two seconds. Their report also notes that an aware, well-trained workforce can reduce the number of employees who fall for a phishing attack to less than 5%.

Monitoring Policies

Shortly after its 2013 breach, Target hired Verizon to assess its networks for weaknesses. The report notes that:

" . . . while Target has a password policy, the Verizon security consultants discovered that it was not being followed. The Verizon consultants discovered a file containing valid network credentials being stored on several servers. The Verizon consultants also discovered systems and services utilizing either weak or default passwords. Utilizing these weak passwords the consultants were able to instantly gain access to the affected systems."

Where were Target's IT management, security team, and internal audit team? Apparently, no one was monitoring one of the basic rules of hardening servers and telecom equipment. Failure of senior management to establish a culture of protecting corporate IT assets resulted in material harm to Target's reputation and financial results. Appropriately, the CEO lost the confidence of the board and was replaced.

Companies should consider using the SANS CIS Critical Security Controls Version 6.0 (at http://www.sans.org/critical-security-controls) as a basis for their monitoring. Some example areas to focus on are:

- Is there an inventory of authorized and unauthorized hardware and software?
- Is all hardware hardened (meaning configured by default to close known security weaknesses)?
- How are administrative accounts controlled?
- Are individual user accounts and their associated roles managed actively and based on least access needed?
- What data is encrypted? At rest? In motion?

An Ounce of Prevention: Vulnerability Testing

In fulfilling its governance responsibilities, the Committee might reasonably request a vulnerability analysis or penetration test by independent consultants. For example, had Target asked Verizon's ethical hackers to attack its company's cyber defenses before their breach, weaknesses would have been identified and perhaps the incident would have been prevented. The findings of an external agent are as significant to the organization's security as audit findings are to its financial and compliance reporting. Demanding an appropriate control environment in the organization is nothing new to boards, although the nature of some security controls probably is. Ensuring that senior management is monitoring and updating key security controls and addressing any findings from external penetration tests will help set the tone for a strong security environment.

THE SANS TOP 20 CRITICAL SECURITY CONTROLS

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capability
11. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Source: *http://www.sans.org/critical-security-controls*

Meeting Three

Assessing Incident Handling Preparations

Meeting Three Overview

One of the primary tasks of the board of directors is to ensure the best possible future for the company. By definition, an organizational crisis is an event that, poorly handled, could lead to impairment or failure of the organization and possibly expensive and distracting litigation. This makes crisis management an important topic for every board and management team. Crises come in many forms, but, until recently, a cybersecurity incident was probably not one that most organizations had on their list of top concerns. Breaches and other cyber incidents are now so common and impactful that every organization must prepare for them.

The question is not if a cyber incident will happen, but rather when and how effectively the company will detect it and respond. The board's proper role here is to make sure that the organization is prepared to effectively handle such an event when it does occur.

For the Committee, there are three topics to review with the CISO:

1. A TRIAGE PROCESS

Particular attention should be paid to the most serious incidents.

- Did they really pose significant business risk?
- How were they detected and resolved?
- What lessons did the security group take from the incident and what actions were taken?

Questions to Consider

- ☐ What is the triage process for potential incidents and how are the categories of severity determined?
- ☐ Specifically, are these determinations based upon the direct financial impact to the business rather than other considerations such as reputational damage? For this, Committee members can refer back to the list of most valuable information assets identified.
- ☐ Once the categories are understood, the Committee should obtain information about how many of each type of incident occurred in the past and how effective detection and responses were.

2. POLICIES FOR HANDLING INCIDENTS

A review of the incident handling policy and process should give the Committee members a sense of how the company intends to handle incidents.

By reviewing the most significant incidents of the past year, the Committee can also judge whether or not the incident response process was consistently followed.

Questions to Consider

- ☐ What are the criteria for informing the CEO? The board?
- ☐ At what point in the process do business decisions need to be made?
- ☐ Who will make them?
- ☐ Are regulatory obligations identified and properly handled?
- ☐ What are the procedures to notify customers and law enforcement?

3. AN INCIDENT RESPONSE TEAM

There should be a standing Incident Response Team and the Committee should ensure that all the key players participate. Beyond security and IT, there should be representatives from compliance, corporate communications, finance, legal, and risk management. Each individual's role should be clearly defined. As noted above, the team should have identified the most significant risks facing the organization and practiced their response to these scenarios through tabletop or live exercises.

An organization with an Incident Response Team that understands the potential risk scenarios and that is well rehearsed in responding to them should significantly mitigate the impact of any breach. After a breach has occurred is not the time to be designing the process. It is incumbent on the Committee to ensure that management is well prepared.

Who's on the Team

- ☐ Security
- ☐ IT
- ☐ Compliance
- ☐ Corporate Communications
- ☐ Finance
- ☐ Legal
- ☐ Risk Management

Conclusion

Cyber risks are relatively new and most board members are not experts in technical aspects of managing them.

This is OK since the directors' role is to ensure that management has resources and robust processes in place to protect the corporation. A standing item on the board's agenda must be a discussion of three topics with the company's CISO and CEO:

Risk Assessment & Accountability

- Does the security team sufficiently understand the business, and have they properly identified the key business risks that could arise from a cyber incident?
- Is strong leadership and accountability evident?

A Culture of Vigilance & Prevention

As with compliance, security requires constant vigilance and good housekeeping.

- Is management attending to these issues, and are they ingrained in business practices at the company?
- How is security being audited?

Plans & Processes for Incidents

- What is management's plan to deal with security incidents as they occur? Are the policies, procedures, roles and team members clearly identified?
- Does security refine its plans after every serious incident or practice exercise?

By focusing on these three topics, the board will build a constructive partnership with management to ensure that proper oversight and due diligence are in place. By working together, a company's management and its board are positioned to protect the interests of owners, customers, employees, and suppliers.
Anything less is unacceptable.

About the Authors

Richard Y. Flanagan

Dr. Richard Flanagan is an Assistant Professor of Management Information Systems and founding Director of the department's M.S. in IT Audit and Cybersecurity (ITACS). ITACS began with 11 full- and part-time students in January 2012 and will welcome more than 100 students this coming fall. Before returning to Temple University, where he got his Ph.D., Dr. Flanagan worked at Rohm and Haas Company (later Dow Chemical) for 29 years. He worked throughout the company in Information Technology, Research and Development, the Legal Division, and the Adhesives & Sealants business. He held numerous global leadership positions and worked in all regions of the world. He led successful projects and teams working in IT infrastructure, applications development, business process consultation, re-engineering, and IT strategic planning. For the last eight years of his tenure he was the IT Director and was responsible for aligning IT's efforts with the needs of the company's many businesses.

Dr. Flanagan holds an A.B. degree in government and law from Lafayette College, an M.A. in criminal justice from John Jay College (CUNY), and a Ph.D. in political science from Temple University.

Janet L. Yeomans

Jan Yeomans is a retired 3M executive. As Treasurer, her focus was on risk management. Recognition that most, if not all, corporate risks have the potential to have material financial impact led her to adopt a broad approach that included whatever could be seen as potentially impacting the company's balance sheet.

Jan graduated magna cum laude from Connecticut College with majors in mathematics and physics. She earned a master's degree in mathematics from Illinois Institute of Technology and an MBA from the University of Chicago.

Currently a resident of Philadelphia, Jan has worked with a number of not-for-profit organizations and with state government.

Fox School of Business
TEMPLE UNIVERSITY®