Cybersecurity

The Board's Role

"There are two kinds of big companies in the United States. There are those who've been hacked...and those who don't know they've been hacked."

JAMES COMEY
FORMER FBI DIRECTOR
(60 MINUTES, CBS)

Boards increasingly understand that cybercrime is a risk management issue that affects the entire organization and requires board oversight. However, although directors know that they need to stay informed about cybersecurity, keeping up with it in the complex, rapidly evolving world of IT is often a challenge. A governance survey of audit committee members found that only 21 percent of directors agree their company has cybersecurity risk well under control — perhaps in part because about 66 percent said their senior IT executive reports to the board only "occasionally"[1].

In response to boards' growing concern about how to approach cybersecurity, Spencer Stuart and Morrison & Foerster convened a panel to frame the board's role in overseeing cybersecurity risk and to help identify key questions directors should be asking — both of themselves and management. The discussion featured Timothy Campos, chief information officer of Facebook and board member of JDS Uniphase; Malcolm K. Palmore, assistant special agent in charge, FBI San Francisco Office Cyber Program; and Steven West, board member, Cisco Systems (audit committee chair) and Autodesk. This article highlights learnings on the board's role in overseeing cyber risk and what they can do to protect their organizations from cyber threats.

[1] 2014 NYSE Governance Services, Corporate Board Member and RSA, in association with Ernst & Young LLP survey of 200 audit committee members.

THE RISK IS REAL

Organizations of all kinds are regularly targeted for cyberattack, and the media report a seemingly never-ending series of breaches. In June 2015, the U.S. Office of Personnel Management disclosed it had been hacked, comprising one of the largest breaches of federal employee data in recent years with roughly 18 million current and former federal employees' personal data potentially at risk of being compromised. The highly publicized breaches of Target Corp. and Neiman Marcus — in which the credit cards and addresses of more than 70 million customers combined were compromised — was part of a long list of major attacks in 2014.

"Cyber threats are very active and growing. There is no doubt perpetrators will continue to target organizations for the purpose of acquiring and monetizing personal data and information as well as the goal of disrupting the business, injuring key corporate stakeholders, and impairing the value of the enterprise," warned Malcolm K. Palmore, assistant special agent in charge, FBI San Francisco Office Cyber Program.

A breach can have dire consequences for companies, including regulatory investigations, loss of intellectual property and financial risk from fraudulent transactions. The greatest risk might be to a company's stature in the eyes of its customers and investors.

As a result, cybersecurity has catapulted to the top of boards' list of concerns. In 2011, Lloyd's of London's biennial Risk Index ranked cybersecurity in 12th place on board agendas. By 2013, cybersecurity had risen to third place. The board plays a crucial role in ensuring that the company is adequately managing its cybersecurity risk. The panelists agreed that the board must appropriately prioritize cybersecurity, and ensure cybersecurity policies and procedures are in place and appropriately funded. As Tim Campos, chief information officer, Facebook and board member of JDS Uniphase stated, "Any company involved in the Internet or storing confidential customer information on their network must include cybersecurity as a priority board focus. The board must ensure that management is equipped to manage the risks from cybersecurity with appropriate knowledge, staffing and budgets."

Our panelists identified five key aspects to the board's role in managing cybersecurity risk.

1. Accept Responsibility for Cybersecurity

Our panelists agreed that how a company and its board approach cyber risk depends on the industry and the company's tolerance for risk. Some boards deal with cybersecurity issues as a whole board, while others choose to delegate these matters to a standing board committee, such as the audit committee, to help facilitate achievement of those goals. However, while the audit committee may be well-equipped to address issues of risk, audit committees are not traditionally oriented towards matters of innovation, competitiveness and strategy — all of which are essential to effective technology oversight. Consequently, a small number of boards (42 S&P 500 companies in 2015[2]) have created a standing technology committee to address these issues.

A separate committee does not relieve the full board of its core oversight responsibilities. Boards must ensure that cybersecurity is viewed as an enterprise risk issue, not just an IT topic, and that discussion of cybersecurity gets adequate time on the board agenda and with management. However, the structured approach of a committee — and the expertise of its members — allows the full board to rely on the committee's recommendations and decisions.

"Delegating cyber risk to a separate committee can help boards facilitate deeper discussions that should be taking place, but aren't possible due to competing agenda items in full board meetings," commented Steven West, audit chair for Cisco Systems and Autodesk director.

2. Set Expectations for Management

Regardless of how boards structure themselves around this matter, directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget to oversee cybersecurity risks.

[2] 2015 Spencer Stuart Board Index

Boards need to ensure that they are adequately briefed about the company's security model and vulnerabilities. Briefings should occur on at least a quarterly basis, and if the management of cyber risk is allocated to a committee, the full board should also be briefed at least semiannually. "Regular briefings are critical, with management demonstrating progress on its security strategy and keeping the board apprised of challenges and changing priorities," commented Campos.

Boards may also want to consider hiring outside experts to explain the latest technologies and best practices to help directors become more educated on cyber risk and preparedness. Existing third-party advisers, including law firms, audit firms and communications firms, may have skilled experts in this area.

3. Understand Your Company's Cyber Risk

Assess legal risk. Boards must ensure that they understand the legal implications of cyber risk. Federal and state laws often require that customers be notified in the event of a breach, and international laws, including privacy practices, may apply to some companies. Companies should have plans in place to deal with these risks. There may also be industry-specific legal concerns. For example, some industries, such as healthcare and defense, must take special circumstances into consideration.

Prioritize assets. Boards should undertake a thorough analysis of the company's most valuable assets and determine the risk that each might present in the event of a cyberbreach or loss. For some companies, assets might include a proprietary database, a chemical formula, a patented manufacturing process or other type of intellectual property. It could be customers' private financial data or competitive research that has been years in the making. A discussion around which risks to prioritize, avoid and mitigate should take place among directors.

"While minimizing risk is an important part of the equation, boards also want to think about technology in the context of the business to consider appropriate tradeoffs between risk and innovation and growth," commented Campos.

Improving Access to Cyber Expertise:

UNDER WHAT CIRCUMSTANCES SHOULD A COMPANY HAVE A SECURITY EXPERT ON THE BOARD?

Spencer Stuart has worked with a growing number of companies to recruit a director who brings technology expertise to the board. To address escalating cybersecurity risk, some boards have brought in a director who comes from a security background. Typically, these companies are at high risk for cyber-attacks and in industries like financial services and healthcare or conduct significant business online. The cybersecurity board member can help the management team make difficult risk management decisions as well as increase the general level of cybersecurity knowledge and awareness on the board. However, the board should not isolate cybersecurity responsibility with just this one board member, but continue to view cybersecurity as a full board priority.

The level of IT savvy a company adds to its board depends on the business. Companies must balance many factors — including need for industry expertise, financial knowledge and sophistication, global experience and diversity — in filling board vacancies. Whether or not a board adds a cybersecurity expert, boards need to ensure that they have adequate access to cybersecurity expertise. Many CISOs provide their boards with regular training on cybersecurity topics, or outside experts can be brought in for board education.

Consider cyber insurance. Does the company's insurance policy cover breaches? Is the coverage equal to the value of the company's assets? Some companies may consider buying dedicated cyber insurance as an additional method to transfer or mitigate risk.

Identify risk from third parties. Third parties — including outsourced IT and other partners — may have vulnerabilities of their own. It is important to factor in the risk associated with partnering with third parties as companies coordinate their cybersecurity strategy.

Anticipate change. Companies are especially susceptible to risks during times of change: when they move into new markets overseas, adopt new technologies with unknown vulnerabilities and bring third-party vendors into the fold. Boards need to be sure that they understand new vulnerabilities that emerge as the organization evolves.

4. Assess Current Cybersecurity Practices

Our panelists identified questions boards might consider when assessing their preparedness:

- Does executive leadership have a clear and consistent understanding of cybersecurity relative to the business?
- Does management understand its responsibility for cybersecurity and have an adequate system of controls in place?
- Is the cybersecurity budget appropriately funded?
- Is the organization's enterprise risk management program appropriately staffed and resourced given the types of risk assessed?
- Are there clear policies and procedures in place in the event of a breach?
- Is the company's disclosure response in line with SEC guidelines and shareholders expectations?

In addition to internal audits and briefings, our panelists recommended hiring an outside auditor to evaluate the company's level of preparedness for a breach. Resistance to bringing in outside consultants is a red flag that the current cybersecurity practices and technologies may need updating. Additionally, having brought in an outside expert can pay off later, in the event of a breach: if you can show on record that you've had experts in, then you have a paper trail documenting your preparedness efforts. Many companies lack the internal security expertise to manage through a cyber-security program. The board plays an important role in mandating the use of outside experts.

5. Plan & Rehearse

Our panelists agreed that when a breach occurs, there will be pressure to move quickly. You will have to make a series of decisions in a matter of hours. Therefore, it is vital to have policies and procedures in place before a breach occurs. "It is critical that the management team and the board have a detailed plan in place," commented Palmore. "In my experience, the most effective responses to a serious security incident come from those organizations that have prepared in advance and even rehearsed."

To prepare for a breach, our panelists recommended boards:

Review management's response plan. Boards should ask to see management's response plan to potential cybersecurity breaches. The plan should identify who will be responsible for making decisions when a breach occurs and what actions the company will take in the event of a breach. Some questions to consider:

- Under what circumstances will there be a public announcement? If so, when?
- Do you need to send notice to your customers?
- Under what circumstances will you call law enforcement?
- In the event of a breach, will you bring in a forensic group? If so, will the forensic team report to the board or management?

Do a tabletop exercise. It may be helpful to do a "dry run" of a breach. The time you invest will help you deal more effectively with an actual breach. Analyze what works and what doesn't, and modify your plan as necessary.

Create a rapid response team. A dedicated team ready to act in the event of a breach helps ensure that your response goes smoothly.

Questions for the Board to Ask of Management

What are the company's most valuable assets?

Has the company effectively allocated resources based on risk appetite and strategic assets?

Is there an enterprise-wide risk management framework in place with adequate staffing and budget to oversee multiple organizational risks including cybersecurity?

What potential vulnerabilities does the company have to its networked environment? Who can connect? Do third parties have access? How is mobile handled?

What technical capabilities does the company have in place to identify malicious events in real time?

What is the company's response plan in the event of a breach/attack? How often is the response plan tested?

What relationships does the company have with government and other third-party organizations to respond effectively to a breach? What relationships need to be developed?

Establish a relationship with law enforcement. If you already have a relationship with law enforcement, you're ahead of the game in the event of a breach. Palmore recommended companies connect with their local FBI field office before a breach occurs. "An existing relationship with your FBI office can save valuable time and resources to help contain the impact of a breach."

CONCLUSION

When it comes to cybersecurity, vigilance is key. Boards must ensure there is executive ownership — ideally at the top with the CEO and that the management team and IT are keeping security top of mind as they make decisions about new programs and products.

Even with the best plans in place, it's important to recognize that cyber risk cannot be completely eliminated.

Breaches are inevitable, but boards can mitigate risk and damages by staying informed and ensuring that, in the event of a breach, their company is prepared to respond.

ABOUT THE AUTHORS

Michael Dickstein is a member of the firm's Technology, Media & Telecommunications and Board Services practices. He specializes in recruiting board members and senior-level executives for technology clients as well as chief information security officers across a number of different industries. Michael splits his time between the firm's Silicon Valley and Seattle offices. Prior to joining Spencer Stuart, Michael was a management consultant with McKinsey & Company and has over 10 years of operating experience as an executive with technology companies.

Based in Silicon Valley, **Jonathan Visbal** is a member of Spencer Stuart's Technology, Media & Telecommunications, Board Services, Marketing Officer and Private Equity practices. He specializes in senior-level and board director assignments in the technology and communications arena, with a concentration on the globalization of businesses via new technologies. Jonathan pioneered Spencer Stuart's entry into clean/green technology, cloud computing and mobile applications. He has served as a member of the firm's board of directors and as the leader of the firm's global Technology, Media & Telecommunications Practice as well as the Silicon Valley office.

SpencerStuart

ABOUT SPENCER STUART

At Spencer Stuart, we know how much leadership matters. We are trusted by organizations around the world to help them make the senior-level leadership decisions that have a lasting impact on their enterprises. Through our executive search, board and leadership advisory services, we help build and enhance high-performing teams for select clients ranging from major multinationals to emerging companies to nonprofit institutions.

Privately held since 1956, we focus on delivering knowledge, insight and results through the collaborative efforts of a team of experts -- now spanning 56 offices, 30 countries and more than 50 practice specialties. Boards and leaders consistently turn to Spencer Stuart to help address their evolving leadership needs in areas such as senior-level executive search, board recruitment, board effectiveness, succession planning, in-depth senior management assessment and many other facets of organizational effectiveness.

For more than 25 years, our Board Services Practice has helped boards around the world identify and recruit independent directors and provided advice to chairmen, CEOs and nominating committees on important governance issues. We are the firm of choice for both leading multinationals and smaller organizations, conducting more than one-third of our assignments for companies with revenues under $1 billion.

For more information on Spencer Stuart, please visit **www.spencerstuart.com**.

Social Media @ Spencer Stuart

Stay up to date on the trends and topics that are relevant to your business and career.

© 2015 Spencer Stuart. All rights reserved.
For information about copying, distributing and displaying this work, contact: permissions@spencerstuart.com.

Amsterdam
Atlanta
Bangalore
Barcelona
Beijing
Bogota
Boston
Brussels
Buenos Aires
Calgary
Chicago
Copenhagen
Dallas
Dubai
Frankfurt
Geneva
Hong Kong
Houston
Istanbul
Johannesburg
Lima
London
Los Angeles
Madrid
Melbourne
Mexico City
Miami
Milan
Minneapolis/St. Paul
Montreal
Moscow
Mumbai
Munich
New Delhi
New York
Orange County
Paris
Philadelphia
Prague
Rome
San Francisco
Santiago
Sao Paulo
Seattle
Shanghai
Silicon Valley
Singapore
Stamford
Stockholm
Sydney
Tokyo
Toronto
Vienna
Warsaw
Washington, D.C.
Zurich

ARCL_CyberSecurity_073115