XCEO INK

April 27, 2016
Volume 11, Issue 2

XCEO, Inc.
www.xceo.net

How The Board of Directors Can Oversee Cybersecurity Risk

Written by Douglas Park, JD, Ph.D.

Article Highlights:

- The IT department is not responsible for overseeing cybersecurity risks but only managing them. Therefore, the board should not pass the cybersecurity risk oversight to the IT department.
- Management should report to the board on: the company's areas of greatest cyber vulnerability; cyber insurance; internal controls; and information gathering systems.
- Enlightened directors should challenge industry standards and consult advisors who can challenge management's assumptions.

Hacking. Data loss. Phishing and malware attacks. These words strike fear in the hearts of most board members for good reason. PwC reports that major cyberattacks grew 38% from 2014 to 2015. The Akin Gump law firm identifies cybersecurity as the third most important topic for boards in 2016 after long-term strategy and shareholder activism. The fast moving, constantly changing area of cybersecurity is technical, confusing, and new. As a result, many boards of directors are unsure of how to effectively oversee cybersecurity risks.

Cybersecurity threats include: (1) hacks and breaches. These have hit companies in every industry, from financial services (JP Morgan Chase), retail (Target), technology (Adobe), healthcare (Excellus BlueCross BlueShield), to law firms (Cravath Swaine & Moore LLP); (2) disgruntled employees stealing sensitive information from the inside; and (3) carelessness, where employees lose laptops and phones or fail to set passwords for their devices. Because no company's cybersecurity system is invincible, the question is when, not if, a company will experience a serious attack.

Unfortunately, the consequences of cybersecurity breaches are significant. The World Economic Forum's 2016 Global Risks Report estimates that cybercrimes will cost $445 million globally this year. That is more than the market capitalization of Microsoft, Facebook, or ExxonMobil. Companies that experience cyberattacks suffer reputational harm and a loss of customer trust. Customer trust is damaged because their personal data and information is exposed, leaving them vulnerable to identify theft and financial fraud.

The Board's Role in Cybersecurity

In the midst of the growing frequency and impact of cyberattacks, the role of boards in overseeing cybersecurity risk is evolving. A survey by NASDAQ and Tanium, whose cybersecurity platform monitors every piece of information in a company, reports that platform monitors every piece of information in a company, reports that 43% of directors cannot understand a cybersecurity report as well as they can understand a financial report. The survey also finds that cybersecurity knowledge is lower among independent directors than executive directors. About 30% of board members do not feel responsible for the consequences of cyberattacks, even though oversight of cybersecurity risks is the board's responsibility. The IT department is not responsible for overseeing cybersecurity risks but only managing them. Therefore, the board should not pass the cybersecurity risk oversight to the IT department.

Action Steps for the Board

To fulfill its responsibility to oversee cybersecurity risk, the board can take three actions:

1. Improve the board's knowledge of cybersecurity.

This can be done through training and education from experts. The board can hire a cybersecurity consultant or add cybersecurity expertise to the board, depending on whether the company is in a high risk industry like financial services or healthcare. The goal is to not make the board member technical experts, but instead to help them become literate about cyber threats and how to read a cybersecurity report.

2. Understand the company's state of cybersecurity.

Management should report to the board on: the company's areas of greatest cyber vulnerability; cyber insurance; internal controls; and information gathering systems. Most importantly, they should add cybersecurity to the agenda of quarterly board meeting and allocate enough time during the meeting to allow the board to understand the company's ability to identify, protect, and respond to cyber threats.

"Unfortunately, the consequences of cybersecurity breaches are significant. The World Economic Forum's 2016 Global Risks Report estimates that cybercrimes will cost $445 million globally this year."

3. Establish an accountability system for cybersecurity within management and the board.

With respect to management accountability, IT should not bear sole responsibility for cybersecurity risk. An effective risk management system should include: (1) internal audit. The internal audit function should design and establish effective internal controls over the cybersecurity system; (2) operations. The COO should work with internal audit to ensure that the internal controls are embedded throughout the company's business processes, (3) human resources (HR). HR should create and enforce policies and procedures that address how employees, vendors, and contractors handle and protect information, and (4) legal. Laws in many jurisdictions require companies to notify victims of a data breach that causes personally identifiable information to be stolen. Companies must include legal considerations in their response plan.

Board level accountability involves answering critical questions. Which committee will have primary responsibility for cybersecurity risk? To what extent will the entire board be involved in cybersecurity? How does cybersecurity relate to the board's role in risk management? Does the company's risk management system need to be strengthened? If so, what areas need to be strengthened – internal controls, information governance, compliance, company policies?

Conclusion

Cybersecurity threats are here to stay, and they will only worsen in their frequency and damage. Legislation that requires companies to disclose cybersecurity expertise on their boards and successful litigation over cyberattacks are likely to come soon. The challenging regulatory and legal environment increases the urgency of boards of directors to understand and act on cybersecurity risks.

About the Author

Douglas Park

Douglas Park is a recognized authority on corporate governance and securities law. He advises senior executives, board members, and investors on the strategic and legal implications of their decisions on these issues. He also provides litigation consulting and expert witness services on complex corporate governance and corporate and securities law matters to in-house counsel and litigators through Quincy Holyoke Advisors, which he co-founded. Doug has been named a Super Lawyer in Business/Corporate Law. He can be reached at douglasypark@gmail.com.

Doug has been an assistant professor of management at the Hong Kong University of Science and Technology, School of Business and Management, where he taught Strategy and Organization Theory and received several citations for teaching excellence. He has also taught at the Stanford University Continuing Studies Program.

He serves as Chair of the American Bar Association's Corporate Social Responsibility Disclosure and Reporting Committee, a Member of the Sustainability and Governance Subcommittee, and a Member of the Evaluation Committee of the BlackRock/NACD Corporate Governance Innovation Challenge. Super Lawyers named Doug a Rising Star in Corporate Governance and Compliance.

Doug holds a JD from University of Michigan Law School, a PhD in Business from Stanford Graduate School of Business, and an AB magna cum laude with highest honors in Sociology from Harvard College.

XCEO, Inc.
2880 Lakeside Drive
Suite 253
Santa Clara, CA 95054

Phone
408.855.0000
Fax
408.855.0004

Chicago Area Office
1415 West 22nd Street
Tower Floor
Oak Brook, IL 60523

Phone
630.684.2222
Fax
630.681.2299

Media Contact
Michelle Ronco
michelle@xceo.net

We're on the Web!
Visit us at:
www.xceo.net

www.boardportalplus.com

About Our Organization

At XCEO, Inc., we believe individual leadership is the driving force for inspiring creativity and ultimately maximizing intellectual capacity. We provide individual and corporate development in the principles of *Extreme Personal Leadership®*. We call this *X-Leadership* and it is the touchstone of our company.

In today's globally competitive world, intellectual property is a key indicator of long-term success. Corporations and individuals are seeking knowledge intensive solutions to sustain a competitive advantage. At XCEO, we offer *Professional Mentoring and Personal Leadership Development* programs, as well as *Corporate Governance and Board Leadership Development* programs, for high-aspiration individuals and forward-looking corporations.

Through our Professional Mentoring and Personal Leadership programs, we assist individuals in developing personal career and development plans to achieve senior executive-level positions. We also support corporations that recognize the need for a broad array of development options for their high-potential employees being groomed for senior leadership responsibilities.

As part of XCEO's pursuit of enlightened corporate governance, we have created *the Enlightened Corporate Governance® Board Performance Evaluation Program* to support boards and directors in their pursuit of excellence. Through our program, we are leading the movement past compliance, toward principled action which maximizes shareholder value. We have designed a set of eight individual and board evaluation exercises which provide an exceptional opportunity for directors to take their boards to a whole new level of effectiveness.

XCEO is a unique research, development and consulting firm. We are committed to excellence and the pursuit of *Extreme Personal Leadership®*. We specialize in inspiration, and endeavor to inspire highly enlightened executives and high-aspiration individuals to pursue maximum personal achievement. We have a leadership team of highly trained and highly motivated colleagues who are eager to serve our clients. Excellence is our goal. We are located in the heart of Silicon Valley and we stand ready to help our clients achieve extraordinary levels of performance and success.