IMPERVA®

E-BOOK

Cyber Security is the Board's Business

Contents

IMPERVA®

Companies must rank cyber risks that jeopardize business-critical assets in the same way they prioritize other vulnerabilities.

KIM DECARLIS, CMO OF IMPERVA AND BOARD MEMBER AT GIRLS IN TECH AND CHILDREN'S DISCOVERY MUSEUM OF SAN JOSE

Five Questions For The Board: Cyber Security Is The Board's Business

By Kim DeCarlis, CMO of Imperva, Board Member at Girls in Tech and Children's Discovery Museum of San Jose, and graduate of Stanford University

Board members have a fiduciary responsibility to establish and govern business policies and practices that drive a company's financial performance and growth. But do they have a comprehensive view of your enterprise's defense posture to assure they are a conscientious steward of the business?

Perhaps in the past they viewed cyber security primarily as an IT responsibility but now realize the challenge extends far beyond the bounds of technology. Corporate boards face elevating legal liability if they fail to adequately govern risk and protect their businesses from cyberattacks.

With so much at stake, are you giving the board the information it needs to make support smart security strategies decisions? Forty percent of board member respondents in the Wall Street Journal CIO Report are dissatisfied with the information they receive from their security teams.

Consider answering the following questions to initiate an ongoing dialogue with board members.

1. *All companies are vulnerable to major data breaches; what are we doing to minimize potential damage, avoid disruption of business operations, and keep our name out of the headlines?*

Given the absence of a common vocabulary or clear standards for cyber risk management and board oversight, this question can lead to best practices for information security management. What lessons can be learned from how peer companies and competitors are addressing the cyber security challenge?

2. *How prepared are we for a cyberattack? What plans do we have in place for threat prevention and detection and incident response and containment?*

The first order of business involves discovering your assets and risks so you can protect your most valuable business data and applications from cyberattacks. This remains a challenge for many organizations: Verizon's annual Data Breach Investigations Report found that nearly 70 percent of companies discover data breaches via a third party, and they typically don't learn of compromises until months after they occurred.

Is there a crisis communications plan that outlines the process for disclosing incidents and sharing information with peers, regulators, law enforcement, shareholders and media contacts? Is the legal team poised to advise and handle reporting requirements?

"The first order of business involves discovering your assets and risks so you can protect your most valuable business data and applications from cyberattacks."

IMPERVA®

3. *How do we effectively protect our "crown jewels"—the valuable digital data and applications that are most critical to our business and most vulnerable to attack?*

Companies must rank cyber risks that jeopardize business-critical assets in the same way they prioritize other vulnerabilities. It's a risk-reward balancing equation that involves implementing tiered security measures designed to focus on the highest-value targets that must be protected since any breach of these assets would significantly harm the organization.

4. *Where on the cyber threat spectrum should our needle point? What is our risk appetite and our acceptable risk tolerance?*

Corporate directors may rely too heavily on people, processes and technologies that do not deliver the concise information linked to key business objectives. Quantify the organization's appetite and tolerance; ensure that the risk strategy is in alignment and sufficient resources have been allocated. Revisit the critical elements that are core to the company's success and ensure they are rigorously protected.

5. *We spend millions of dollars on cyber security every year; what are the highest-priority initiatives the board should support to stay ahead of adversaries?*

The organization's risk tolerance must be clearly communicated across the enterprise. All employees need to know specifically what falls within and outside acceptable boundaries. Embedding cyber security awareness across the organization encompasses training employees and ensuring they are familiar with security policies and demonstrate secure behaviors regarding system and data access.

If you continuously ask these questions, not only will your board's cyber security literacy dramatically improve, so too will the partnership between IT and the board. When corporate directors and information security leaders understand each other's language and engage in a business-focused dialogue, they dramatically improve their ability to collaboratively develop and implement risk management strategies and technologies that will protect the enterprise and sustain marketplace success.

Cyber breaches can have material impact on an enterprise's financial condition. Finally, it has now become an important business continuity concern.

CRAIG SHUMARD, FORMER CISO OF CIGNA

Why Directors Need To Be Concerned About Cyber Security

Craig Shumard, recognized thought leader and spokesman in the area of information protection.

Craig has dedicated more than two decades to protecting private, sensitive and confidential information as Chief Information Security Officer of CIGNA Corporation from May 1999 until his retirement in 2010.

Directors need to be concerned about the enterprise cyber security posture because of their fiduciary responsibilities. Boards of Directors (BoD) have responsibilities to the National Association of Corporate Directors (NACD) and the Security and Exchange Commission (SEC) for the oversight of cyber security measures and cyber security breach disclosures. More importantly, cyber breaches can have material impact on an enterprise's financial condition. Finally, it has now become an important business continuity concern.

As recent cyber events have demonstrated, security and privacy breaches (e.g., SONY) can have significant and material financial impact to an organization. In today's world, it is not if you will be breached, but rather when and how big the breach will be. Every organization needs to be prepared. BoD governance and oversight is not only warranted, it is necessary.

1. Drivers for effective security governance

There are several drivers that require the need for more BoD governance over cyber security. Specifically:

- Increase regulatory scrutiny over cyber risks demanding explicit and implicit BoD governance
- Proliferation of cyber threats such as the theft of personal information and intellectual property, denial of service attacks, and last but not least, malware infestations
- Growing amount of damages caused by cyber breaches or incidents

Cyber breaches are not only disruptive to the business, they are very expensive to mitigate. They can have a material financial impact to an organization and cause major business disruptions.

CRAIG SHUMARD

2. Fiduciary Duty Compliance

The NACD recommends BoD governance over cyber security. Specifically, NACD recommends the following for cyber security oversight practices:

- Place information security on the board's agenda
- Identify information security leaders, hold them accountable, and provide support for them
- Ensure the effectiveness of the corporation's information security policy through review and approval
- Assign information security to a key committee and ensure adequate support for that committee (usually the Audit Committee)

Boards of Directors are also held responsible by the SEC for oversight to disclose cyber incidents or breaches and their impact.

Laws and regulations designed to force improvement in organizational governance over cyber risks, controls, and their related sanctions and fines are BoD concerns. HIPAA security and privacy regulations for the healthcare industry, PCI security requirements for enterprises processing credit card transactions, and FFIEC regulations for the financial sector over their information processing infrastructure are just the start of a long list of examples.

3. Increasing Cyber Threat Landscape

Cyber threats have also increased the need for BoD governance over cyber security. The major cyber threats include:

- Cyber espionage that result in loss of personal identifiable information or intellectual property. (It seems like the rogue governments are trolling everywhere and everyone these days.)
- Cyber hacktivism such as the Anonymous group dedicated to a variety of social protests
- Cyber assaults like the Distributed Denial of Service (DDoS) attack Sony suffered in 2014

Examples of risks associated with cyber threats include:

- Compromised customer data
- Diminished brand and reputation
- Loss of investor and consumer confidence and loyalty
- Stolen sensitive intellectual property
- Compliance and regulatory sanctions
- And last but not least: Business disruptions

The bottom line is that cyber threats and breaches are increasing in complexity, frequency, and magnitude. No company is immune.

4. Increasing Cyber Breach and Incident Impact

The financial impact to an organization as the result of a cyber breach or incident is also increasing and often material to an organization.

Take the following reported cost associated with some notable recent cyber security breaches: $162M for Target, $63M for Home Depot, $339M for the Office of Personnel Management (and that was for identity theft coverage only), and $171M for SONY.

Cyber breaches are a business continuity concern. The SONY breach highlighted above not only caused a significant business interruption to their PlayStation business, but it also impacted their ability to report their year-end financial statements because many of their accounting systems had been destroyed by malware infiltrated by the hackers. It took SONY months to recover and restore those systems.

In other words, cyber breaches are not only disruptive to the business, they are very expensive to mitigate. They can have a material financial impact to an organization and cause major business disruptions.

Conclusion

Enterprises face cyber threats and attacks every day. In fact, it is not a situation of if a cyber breach will occur, but when and how significant the breach will be. A single cyber security breach can materially affect the financial condition of any enterprise or cause a significant business disruption. As such, BoD governance and oversight over the cyber security posture of the enterprise is not only needed, but required.

A corporate board needs to be responsible for ensuring that an organization's intellectual assets as well as customer information are protected.

ALLAN R. TESSLER, ESQ.

Q&A INTERVIEW WITH EXECUTIVE ALLAN TESSLER

Corporate Directors Must Be Involved in Cyber Security

Mr. Allan R. Tessler, Esq. is currently Director of online brokerage firm TD Ameritrade, and lead Director and Chair of the finance committee of L Brands, Inc., parent company to the Victoria's Secret, PINK, Bath & Body Works, La Senza and Henri Bendel consumer brands. Allan was also Chairman of the Board of Epoch Investment Partners, Inc.; Board Member and chairman Emeritus of the Hudson Institute; and member of the Board of Governors of the Boys & Girls Clubs of America.

Why is it important for corporate directors to understand cyber security risks?

A corporate board needs to be responsible for ensuring that an organization's intellectual assets as well as customer information are protected. Customer data is one of the primary sets of information that needs to be safeguarded from hacking and invasion because of the potential mal-use of that information.

What are the costs of poor board oversight of cyber security risks?

The impact of cyber breaches is quite well known. In the retail world Target had problems, while in the healthcare world Anthem was victimized. A number of banks and brokerage firms have had customer accounts looted of money, while others have lost the identities of their customers. All of this is registered very clearly on the minds of public company corporate directors.

How can corporate directors with no technology background learn to understand cyber security risks?

In order to obtain adequate knowledge, directors have to turn either to other people on the board with technological capability or to people inside management – the COO, the CIO, or the CISO. They also need to discuss these issues with company legal counsel, both internal and external.

What's a basic first step directors could take to ensure effective cyber security?

Corporate directors – the board and management – need to prioritize the intellectual informational assets they have. They need to prioritize the level of protection around these assets relative to their importance to the business and the board, as well as to customers or other communities interested in protect- ing that type of asset. This is a fundamen- tal task of internal analysis that needs to be conducted in every business.

Should every board have a cyber security expert? How about a technology committee?

There are a lot of different approaches. Some businesses get reports from the CIO or CISO. Other companies have a technology committee. In the boards I'm involved with, I have instituted a program where the CIO, the COO, and the CISO either collectively or individually come to every board meeting and address whatever is on their agenda regarding cyber security.

Should corporate directors rely on external audit firms for cyber security awareness?

It's a combination. In two of my boards, we have an outside auditing group come in and review the activities of our cyber security group. They review it on a periodic basis and report back to us. Some businesses I know have retained outside experts either on their risk committee or audit committee to further aid the boards in understanding the performance of their internal activities. Either approach is reasonable.

Are there resources available for corporate directors to better understand cyber security threats?

They can review material on cyber security from director advisory services, law firms or accounting firms. And if the company has engaged an outside cyber security firm, the board can have experts from that firm periodically brief it on how things are going. Getting their viewpoint can be valuable because most of the time boards only hear from corporate insiders.

Learn More about Cyber Security

For more information on cyber security, please visit imperva.com.

For guidance on the role CIOs and CISOs can take in communicating with board members, read the e-book Cyber Security Board Oversight: Taking Ownership of Cyber Security Risks.

IMPERVA

Cyber Security is the Board's Business-1016-rev1