IMPERVA®

E-BOOK

Cyber Security Board Oversight: Taking Ownership of Cyber Security Risks

Table of Contents

Introduction

In 2015, businesses saw a significant increase in the number of new cyber threats. From the controversial dating site Ashley Madison to the cellular giant T-Mobile, no company or industry has remained immune to the advanced, persistent, and sophisticated attacks perpetrated by modern cyber criminals. Enterprises will need to be increasingly proactive and vigilant about their cyber security in order to protect themselves from data breaches and other malicious events.

Enterprise-level cyber security solutions require more than just technology and employee training; they require the top-down involvement of everyone within the organization, including the Board of Directors. Getting buy-in from a Board of Directors is not always easy, however. In this eBook, CEOs and CIOs will discover new ways to educate their Board of Directors and get them onboard with their cyber security.

Why Your Board of Directors Should Care About Cyber Security

It's not always easy for top decision makers to understand why they need to be involved in the process of securing and improving upon their network systems; to them, it may seem like something that needs to be handled "by IT." But cyber security today is a core business operation—and a data breach could have significant and long-lasting consequences. In this section, we will take a look at some of the reasons why your Board of Directors should care about cyber security.

The Board is Accountable for Regulatory Compliance

The Security and Exchange Commission (SEC) holds an enterprise's Board of Directors responsible for overseeing the reporting of cyber-attacks. If these compliance requirements are not met by the organization, they can result in severe fines, penalties, and legal consequences. With the Board of Directors being directly responsible for cyber security, it only makes sense that they be involved in the process. HIPAA, PCI, and FFIEC regulations all demand certain levels of regulatory compliance regarding enterprise cyber security. ***Consequently, the National Association of Corporate Directors now recommends that the Board of Directors maintain governance over cyber security.***

Cyber Threats Are Increasing in Volume and Intensity

Organizations today are subjected to a larger number and variety of cyber threats than ever before. A study by the CyberEdge Group found that 76% of respondents had experienced a successful attack in 2015, which is up from 62% in 2014. Modern cyber threats may be targeted towards compromising customer data, harming a company's reputation, stealing an organization's intellectual property, or even engaging in a social protest.

To make this situation more complicated, companies today also have a vastly expanded attack surface. The Internet of Things and mobile devices have made it more difficult to manage both incoming threats and outgoing data. In fact, the CyberEdge study found that nearly 65% of respondents had experienced some sort of mobile attack in the past 12 months.

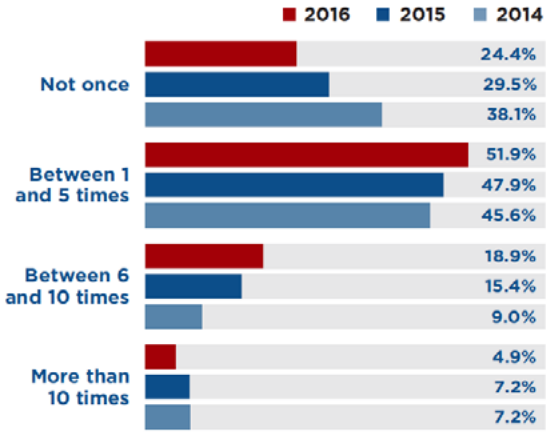


Figure 3: Frequency of successful attacks in the past 12 months.

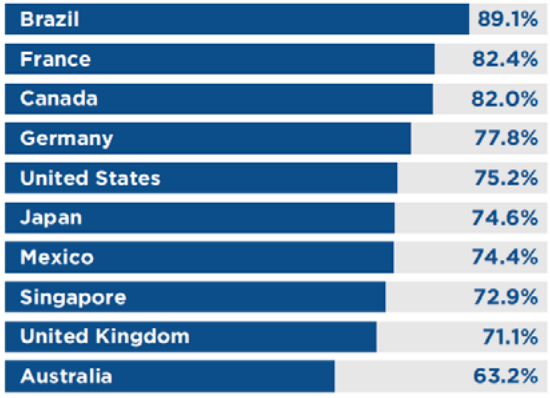


Figure 4: Percentage compromised by at least on successful attach in the past 12 months.

Source: 2016 Cyberthreat Defense Report

IMPERVA®

The Financial Impact of Cyber Breach Is Growing

It isn't just that cyber security attacks are increasing in volume; they are also increasing in damage. Cyber breach attacks are more harmful than ever. Within the past few years, companies such as Target and Sony lost millions of dollars in damages following a data breach attack. According to a report from the Ponemon Institute, the estimated cost of a data breach attack today is $154 per record, with some industries experiencing losses much higher. The average total cost of an enterprise level data breach is about $3.79 million, with attacks costing some businesses significantly more.

This analysis doesn't take into consideration the more lasting financial impact of a cyber security breach; the loss of:

- Customer faith
- Retention
- And brand reputation

The average total cost of an enterprise level data breach is about $3.79 million, with attacks costing some businesses significantly more.

In many cases, it isn't about whether or not a breach attack will occur; it's about how much damage it will do when it does. Risk mitigation and disaster preparedness will reduce the financial and intangible burdens associated with a data breach attack.

It must be impressed upon the Board of Directors that data today is an essential business asset—and that the breach or loss of this data will have serious ramifications for the organization. Consequently, cyber security initiatives need to be considered on all levels of business operations. Of course, that doesn't mean that each member of your Board needs to take a refresher course on the IT profession. There are certain things that the Board of Directors do need to know—and others that they don't.

Risk mitigation and disaster preparedness will reduce the financial and intangible burdens associated with a data breach attack.

IMPERVA®

What Does Your Board Need to Know About Cyber Security?

Where do your cyber security initiatives fit into your enterprise in terms of overall business objectives? What are the major risks that your organization will potentially face—and how prepared is your organization to face them?

An enterprise's Board of Directors needs to understand cyber security insofar as it relates to the decisions that they make to protect and develop the company, its investors, its employees, and its customers. They may not need to know the raw data or the specifics behind the technology, but they do need to be educated regarding any decisions they make that could potentially affect business outcomes.

Measures the Organization Has Taken in Terms of Cyber Security

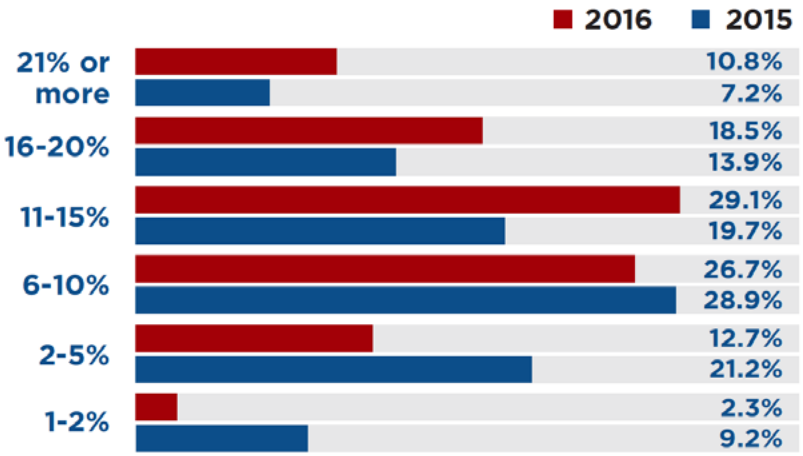
It's important for the Board of Directors to understand that all organizations are under the threat of cyber security breach. The Board needs to be briefed on what steps have been taken to mitigate these threats, from data backup and protection initiatives, to employee training and technical support. The Board should be aware of all of the measures that the organization has taken thus far to improve upon its cyber security and to limit its risk.

The Organization's Current Level of Cyber Security Preparedness

The Board of Directors should be given information regarding where the organization stands in terms of cyber security preparedness, both in relation to where the organization would ideally be and where the organization falls within similar enterprises. ***Cyber security preparedness may seem like a nebulous concept to the members of the Board; they need to understand how prepared the business is even if they do not understand the technologies.*** Benchmarking between the organization's current status and past status is an excellent way to show improvement.

Current Risk Factors and Vulnerabilities within the Organization

When it comes to cyber security, ***it is not possible to entirely avoid risk–only to limit it.*** The Board of Directors should be aware of any current risk factors and potential vulnerabilities and challenges facing the organization. This will give them information that they can use to prioritize spending and create new cyber security initiatives. Risk factors can include everything from legacy products and third-party solutions to the organization's industry.



What percentage of your employer's IT budget is allocated to information security (e.g., products, services, personnel)?

Source: 2016 Cyberthreat Defense Report

Steps Taken to Protect the Organization's Critical Data Assets

Many modern companies rely upon their critical data assets not only for day-to-day operations but for continued success.

The Board of Directors should know
- What data needs to be given top priority
- What steps need to be taken to protect that data, from authentication protocols to backup procedures

Not only will this impress upon the Board the importance of these assets, but it will also give them a better picture of where the organization stands in terms of preparedness.

Once your Board of Directors has the necessary information at hand, they can make educated and timely decisions regarding your organization's cyber security future. Without the above base of understanding, your Board may not understand why these initiatives are important or may fail to give cyber security the priority that it needs to have. Of course, understanding doesn't necessarily guarantee engagement–that may need some additional work.

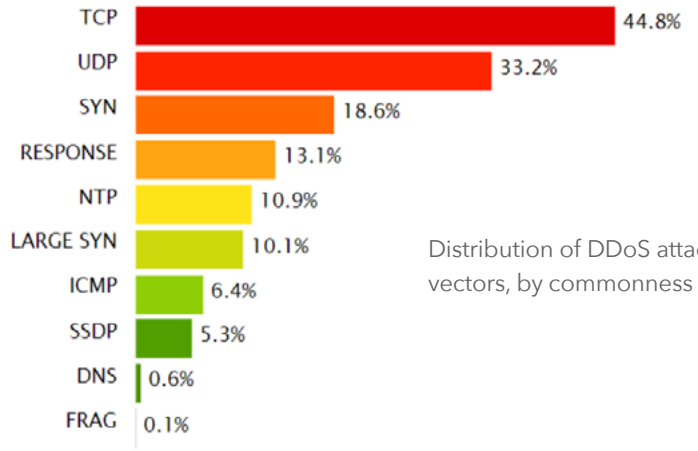
Many modern companies rely upon their critical data assets not only for day-to-day operations but for continued success.

How to Engage Your Board About Cyber Security

For most organizations, there is an endless litany of issues, challenges, and opportunities presented to the Board of Directors at any given time. Keeping the Board engaged and interested in cyber security can become a task in itself—especially when everything is operating smoothly. As any CTO or CIO knows, no one thinks about network security or the system infrastructure until something has gone wrong. ***Engagement is and must be a constant process that continually reminds the Board of Directors of the importance of maintaining their cyber security initiatives.***

Present Timely Status Reports to the Board

Status reports should be presented to the Board of Directors on at least an annual basis. These should include any current cyber security initiatives, the year-over-year improvements, and the organization's current position regarding modern cyber security standards. These timely status reports will update the Board regarding any improvements that need to be made and will show the Board what the cyber security department has been prioritizing. Opening the doors of communication is incredibly important; otherwise cyber security may be drowned out amidst other concerns.



Distribution of DDoS attack vectors, by commonness

IMPERVA

Disclose Risks and Challenges with Strategies and Resolutions

One of the first questions a Board of Directors will often ask when disclosing a strategy is "How can we resolve this?" A failure to answer this question could easily let a serious problem sit on the back burner. Even if the Board of Directors wishes to resolve a problem, they are not likely to have the technical acumen to make their own suggestions. Instead, to keep them involved, you should ***always present your strategies and resolutions alongside any issues that you introduce.*** This will encourage your Board of Directors into making a prompt decision regarding the safety and security of the network. By making it easier for your Board of Directors to be involved you also make it more likely.

Align Security with Critical Business Objectives

It can often become necessary for the Board of Directors of an organization to focus primarily on their own business objectives. This type of "tunnel vision" is often important to the operations of the business, but it also requires that you show exactly how your cyber security initiatives will tie into better business, but it also requires that you show exactly how your cyber security initiatives will tie into better business outcomes, whether it be through damage mitigation or increased internal efficiency. ***Consider where your cyber security initiatives will provide better direct results for the organization in addition to simply improving security.***

A Board of Directors is generally composed of extremely talented, strong-willed, educated, and intelligent individuals. A lack of engagement doesn't necessarily betray a lack of interest, as it might when dealing with employee cyber security training. Instead, the Board of Directors may have members who simply aren't current on their understandings of modern cyber security or who feel as though their attentions are better spent elsewhere. Your goal when engaging your Board of Directors is to present them the information that they need to remain involved. Once you have done so, it's simply an issue of maintenance.

Keeping Your Board Involved With Cyber Security

But what happens if your Board of Directors loses interest in your cyber security initiatives? Support from the Board of Directors can fail for a variety of reasons, though all is not lost. By addressing these issues head on, you can often get everything on track once again.

Don't Get Too Forceful With the Risks

Data breaches and malicious attacks are incredibly hazardous to organizations; they can cause long-lasting financial problems in addition to destroying the branding of a business for some time. ***Nevertheless, repeatedly emphasizing these risks to a Board of Directors can potentially backfire, as they may feel as though the perceived risks have not materialized and are thus exaggerated.*** It's important for any CIO or CTO to present a well-rounded but not alarmist picture of modern cyber security. The more the Board feels that the issues have been exaggerated, the less likely they are to take cyber security issues seriously.

Always Deliver a Structured Overview of Cyber Security Initiatives

A Board of Directors often expects to see extremely detailed and methodical planning when it comes to new business initiatives. For a CIO or CTO to connect with the Board, they must be able to create comprehensive, disciplined, and structured reporting, in addition to developing very clear plans for the organization's development and future. Otherwise the Board of Directors may not feel as though initiatives are ready to implement or feel that your organization is not ready for significant shifts in security.

Give Your Board a Basis for Comparison

Without a solid basis for comparison, a Board of Directors simply can't determine whether the security of their organization is "good" or "bad." The only reliable way for a Board of Directors to see whether their organization is improving or is up to modern standards is to ***compare an organization with prior year benchmarks and leading competitors.*** This will give the Board of Directors something far more real and tangible to hold on to, rather than abstract communications regarding modern technology and security initiatives.

Keep Your Cyber Security Initiatives Grounded

As noted, it's important to always wrap up your cyber security initiatives in business outcomes; if you can't show a clear, positive outcome for these initiatives, it probably won't be considered a priority by the Board of Directors. Cyber security initiatives improve upon business outcomes in many ways, from increasing the peace of mind of investors to protecting the business against potential liabilities. ***When an initiative is either examined or presented, the direct value that initiative has with the company should be included.***

There is a natural ebb and flow to issues that are presented to any Board of Directors; though your cyber security initiatives may be the priority one day, you can also find them sidelined when other critical events are occurring. The most important thing as a CIO or CTO is to remain a patient advocate of your cyber security challenges and priorities. As long as you continually make the effort to educate and engage your Board of Directors, you should be able to create an environment that reliably fosters your cyber security efforts.

Conclusion

An effective cyber security program absolutely requires the support and engagement of your Board of Directors. Without the Board, cyber security initiatives will not be given priority, regulatory compliance may not be met, and an organization will quickly fall behind. Worse yet, data breach attacks can strike at any time—and the consequences of an attack are often disastrous. By impressing upon your Board of Directors the importance of cyber security in the modern arena, keeping the Board educated and involved, and creating a top-down culture of security, you can manage potential risks and develop a proactive rather than reactive security posture that will protect you against many of today's threats.

An effective cyber security program absolutely requires the support and engagement of your Board of Directors.

For More Information

Here are some additional resources to help you get your Board of Directors more involved with cyber security:

Why Directors Need To Be Concerned About Cyber Security

Cyber Security Is the Board's Business: The Top Five Questions Every Corporate Director Should Ask the CISO

Strategies & Tactics to Engage the Board of Directors About Cyber Security