THE EXECUTIVE'S CYBER SECURITY PLAYBOOK

HOW C-LEVEL EXECUTIVES CAN CONTRIBUTE TO A STRONGER SECURITY POSTURE

AUGUST 2016

FireEye

CHAPTER 1

INTRODUCTION

Cyber security awareness is growing as more businesses learn that their networks are vulnerable to an attack. The emerging consensus is that the IT department alone cannot handle security; all employees, especially C-level executives, have a part to play. In fact, executives are responsible for not only the security of data in their departments but also broad employee adoption of cyber security best practices.

For a chief information security officer (CISO), cyber security is obviously job one. A chief information officer (CIO) might list cyber security as one of their top three priorities. Of course, the chief executive officer (CEO) is responsible for everything. And though they may not realize it, every other C-level executive also has responsibilities that play an important part in cyber security posture in their department.

"[Executives] have to figure out what really matters to them," says Kevin Mandia, Chief Executive Officer of FireEye. "What are the critical assets to protect and what are the threats that are intolerable?"

In this ebook, FireEye explains why senior executives must be more proactive about cyber security — before, during and after an event — and how they can help create and maintain a strong security posture.

CHAPTER 2

THE GROWING RISK

The cyber security risk has grown to the point where breaches are inevitable. In 2015, 38% more security incidents were detected globally than were detected in 2014, according to International Data Group Inc. (IDG).[1]

Breaches are also getting more expensive. The average financial loss per breach topped $15 million in the United States in 2015, up from $12.7 million in 2014 and $11.6 million in 2013, according to a Ponemon Institute survey released in October 2015.[2] The figures are based on a survey of 252 companies in seven countries; the U.S. reported the highest breach costs.

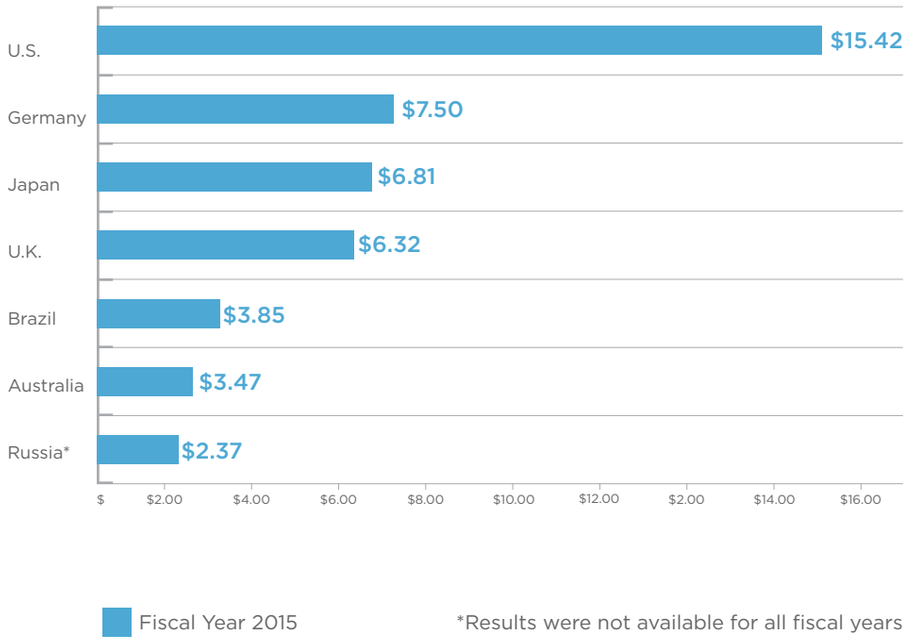
The risks vary by industry. For an electrical utility, the top cyber security priority is keeping the lights on by preventing cyber attackers from disabling the power grid. For a retailer, it's protecting credit card records and customer data. For the aviation industry, it's protecting the air traffic control system for the safety of passengers and flight crews. You need to develop a cyber defense plan that is relevant to your industry.

Executive interest in attending to cyber security is trending in the right direction. The 2015 Global Megatrends in Cybersecurity report, conducted for Raytheon Co. by Ponemon, revealed that the percentage of government and business leaders who consider cybersecurity to be a competitive advantage would likely double from 25% to 51% in the next three years.[3]

C-level executives are taking other steps to become more proactive on cyber security. Mandiant, a FireEye company, regularly conducts Response Readiness Assessments and Tabletop Exercises with information security (IS) and IT staff at client companies to see how they respond to a simulated attack in order to prepare for a real one. Over the last 12 months, these exercises have started to include C-level executives.

"It was really customer driven," says Matthew Shaffer, Principal Consultant for Mandiant Consulting, of the shift. "The idea that breaches are inevitable is finally starting to sink in."

Figure 1: Total cost of cyber crime for 252 companies sampled across seven countries. Cost expressed in U.S. dollars (000,000).



[1] "The Global State of Information Security Survey 2016." International Data Group Inc.

[2] "2015 Cost of Cyber Crime Study: Global," Ponemon Institute. October 2015.

[3] 2015 Global Megatrends in Cybersecurity. Ponemon Institute, February 2015.

CHAPTER 3

SECURITY OBLIGATIONS BY ROLE

In traditional, strictly hierarchical organizations, executive roles were relatively distinct and easy to define. But today, with more nimble organizations and flexible, collaborative roles, responsibilities and interactions can become more complex. Ultimately, however, all C-level executives share a common obligation to support a stronger cyber security posture. Each C-level executive has a unique perspective and contribution to make:

CEO: CHIEF EXECUTIVE OFFICER

The CEO is responsible for the overall management of the company, its strategic vision and direction. As such, the CEO coordinates with the board of directors to set the overall tone of attentiveness to security, and works with the CISO to implement an approach that makes security a key business priority. A 2014 report by the management consulting firm Bain & Co. stresses that CEO support for cyber security is more important now than ever: "Too many organizations fail to align their IT-security capabilities with the company's larger goals and appetite for risk."[4]

[4] Syed Ali, Vishy Padmanabahn and Jim Dixon (Bain & Co.) "Why Cyber Security is a Strategic Issue." 2014.

CIO: CHIEF INFORMATION OFFICER
CISO: CHIEF INFORMATION SECURITY OFFICER

Some organizations have a CISO dedicated to cyber security but sometimes a CIO handles corporate cyber security as well as the company's internal information technology services. The CIO and CISO roles have gained visibility and responsibility in the wake of increased numbers of breaches. This executive works closely with other C-level peers and line-of-business leaders to increase cyber risk awareness and to determine and help meet cyber security needs across the organization.

CTO: CHIEF TECHNOLOGY OFFICER

The CTO owns the vision and roadmap for the organization's products and services, and should add security considerations to the development, review and approval processes. Ideally, the CTO and CISO should consider collaborating closely to inspire one another and ensure comprehensive, technically rigorous cyber security for the company's products.

CFO: CHIEF FINANCIAL OFFICER

The CFO is responsible for the company's finances and financial reporting. As such, the CFO should establish strategic security priorities to secure financial systems, determine the business risk associated with breaches, and evaluate the cost of breach remediation. Working with the CEO, CISO and other executives, they help to appropriate and allocate cyber security funding as priorities dictate.

COO: CHIEF OPERATING OFFICER

The COO makes sure the company has the proper operational, administrative and reporting systems in place for optimal operating efficiency.[5] They often also take point on legal and regulatory compliance across the entire organization. By working with the CISO, they support the proper establishment, maintenance and documentation of organizational security.

CCO: CHIEF COMMUNICATIONS OFFICER
CMO: CHIEF MARKETING OFFICER

This executive role includes functions for identifying, informing and acquiring customers. Some companies even refer to this executive as a Chief Customer Officer. The CCO serves as the bridge between the public, customers, partners, other stakeholders and the company in the event of a breach. Meeting those demands requires pre-planning in close consultation with the CISO. During an attack, the CCO maintains an open line with the CISO to enable rapid intra- and extra-company communications that protects customers, business interests and the corporate brand.

[5] Society for Human Resource Management.

CHRO: CHIEF HUMAN RESOURCES OFFICER

Because the CHRO focuses on legal, regulatory, and communications issues related to the workforce, they are critical to all discussions concerning breach preparedness. By working with the COO, CCO and CISO, they can ensure that employee records are properly protected. In the event of a breach, they should disseminate timely information to managers and internal communications staff to better protect the privacy, identity and assets of affected employees. The importance of this role cannot be understated, given that the director of the U.S. Office of Personnel Management (OPM) was forced to resign after 21.5 million government employee records were stolen from the OPM in a breach made public in June 2015.

CPO: CHIEF PRIVACY OFFICER

In many U.S. states and foreign countries, laws dictate security requirements for personally identifiable information (PII), including notification requirements when PII may be compromised. As a CPO develops and implements policies designed to protect employee and customer data from unauthorized access,[6] they work hand-in-hand with the CISO, CCO, COO, CHRO and CEO. With a strong legal background, accessible personality, and technology awareness the CPO ensures a focus on the personal side of security.

Although each executive has specific security needs, organizational security is only as strong as its weakest link. The ability to implement a strong security posture across the entire organization is directly correlated with how competently they collaborate and coordinate their activities before, during and in the aftermath of an attack.

...organizational security is only as strong as its weakest link.

[6] Margaret Rouse (Tech Target). "Chief Privacy Officer (CPO) October 2014.

CHAPTER 4

ETERNAL SECURITY VIGILANCE

While security is something that employees of a company or other organization need to be vigilant about every day, there are specific cyber security best practices that executives should adopt before, during and after a breach.

BEFORE A BREACH

Preparing for a breach should be part of the daily security routine of any organization. Multiple layers of network security minimize gaps in protection. In addition to firewalls, intrusion prevention and antivirus technology, you should also consider deploying advanced intelligence capabilities that inform you of emerging threats beyond your own network perimeter. Persistent security measures will also help protect off-premise and remote devices, such as cell phones and tablets.

Because the cyber threat landscape is always changing and new security solutions come to market all the time, your organization needs to review its security strategy regularly. The U.S. Department of Homeland Security (DHS) has released a list of five questions companies should ask themselves to assess their cyber risk:

1	2	3	4	5
What is the current level and business impact of cyber risks to our company? What is our plan to address those risks?	How is our executive leadership informed about the current level and business impact of cyber risks to our company?	How does our cyber security program apply industry standards and best practices?	How many and what types of cyber incidents do we detect in a normal week? At what point are executives notified of incidents?	How comprehensive is our cyber incident response plan and how often is it tested?

"Cyber security is not simply about making a checklist of requirements," the DHS explains. "Rather, it is managing cyber risks to an acceptable level."

Preparing for a cyber attack involves developing a coordinated response plan that considers every possible threat to your organization. Studying security best practices — and failures — of other companies, especially those in your same industry, is an excellent first step. In addition, discussions and workshops with counterparts — in finance, human resources, marketing, etc. — at other companies helps identify pertinent threats and develop defenses. And, like fire drills at school, the response plan should be tested frequently and revised and improved as needed.

"The worst time to engage in a fire drill is the first time there's actually a fire," says Shaffer. To help their clients, Mandiant Consulting experts conduct and guide tabletop exercises — mock scenarios of cyber attacks on the client company. Along the way, Mandiant consultants add "inserts" — like plot twists in a movie — introducing new developments in the scenario. Now your web site has been defaced. Now the attackers have accessed confidential records. Now they are removing sensitive data from your network. Participants go through the process of discovering, identifying, prioritizing and addressing issues, as they would in a real attack. In more recent exercises, executives have taken a more active role to gain practical experience involving breach events.

Beyond just developing an incident response plan, executives must practice ongoing cyber risk management, the DHS advises. That means continuously monitoring the risk environment as well as reviewing IT budgets, new technologies and services, security spending, incident reports and company policies that have security implications.

Penetration and red team testing help establish the actual state of your security systems and procedures — not just what they look like on paper. These assessments thoroughly review your security environment, and create and execute realistic threat scenarios against your vulnerabilities that your security teams must then respond to.

ASSESSMENTS: BE PREPARED FOR A BREACH

Several cyber security assessments can determine how you can most effectively prepare for and respond to inevitable attacks:

Compromise Assessments apply extensive threat intelligence and security expertise to determine whether you have been breached in the past, or are currently under attack. This assessment includes recommendations for further investigation, containment, and long-term security improvements.

Proactive Objective-Based Tests evaluate your security measures against the tools, tactics and procedures used by attackers who typically target your industry. Penetration testing, red team operations and other objective-based tests can detail risk, probability of exploitation and potential business impact, and provide actionable recommendations.

Security Program Assessments review your security organization, practices and procedures against the latest industry standards in 10 critical security domains. This comprehensive assessment provides a security program roadmap with prioritized recommendations to close gaps based on vulnerabilities, attack trends, and any likely malicious activity in your systems.

Response Readiness Assessments review your security operations and incident response capabilities for detecting and responding to attacks. The final deliverables include a security roadmap with prioritized recommendations.

DURING A BREACH

All that advance planning and those security drills are put to the test when an incident actually occurs.

Your organization's incident response team must spring into action when they identify a breach. They need to determine where the attackers are, what they seem to be after, how far they have advanced and how long they have been in your systems. They can then block the attacker to prevent further losses and mitigate any damage. You also have a role to play in the response. As you work with your CISO, you may want to contract security consultants to advise you on incident response. Such experts may be aware of newer and evolving security threats and have the knowledge, technology and skill to defend against those attacks.

Just as important as responding to the attack is deciding how to disclose the incident to the outside world. Keeping the breach quiet may no longer be an option, given legal disclosure requirements and the likelihood that news of the event will become public.

"If you're breached and you know it, somebody else knows, too," says Mandia. "You are in an absolute foot race to get your arms around what happened and what you are doing about it."

Somebody else is likely to know about your breach first because in only 47% of breach incidents studied by Mandiant Consulting did the targets discover the breach on their own. In 53% of cases, the alert came from others, such as a partner or law enforcement agency.[7]

However, you have to be careful about what you disclose, to whom and when. Some companies opt to disclose as much as possible out of a sense of corporate responsibility. Having a communications plan in place ensures that you release only relevant information to the correct authorities and the general public in a timely manner, using appropriate channels. It's important to work with your legal counsel as well as your public relations partners to determine not only how to put the best foot forward to customers, suppliers, employees, and the public, but also to determine what's required of you under relevant laws.

There are also situations in which there can be internal disagreement about when and what to disclose. Shaffer says there have been instances where legal counsel for the company says there are specific rules from regulatory agencies that notification of a breach must occur within 24 or 48 hours of the incident. But the public relations team may also want to proactively notify the public via news media, even if it's not legally required. Who gets notification first, Shaffer asks, the regulators or the media?

While disclosure decisions are important, the larger concern during a breach is to gain control of the situation, remove attackers from your network and get operations back to normal as soon as possible. Internal coordination with your legal counsel and public relations department is key.

Internal coordination with your legal counsel and public relations department is key.

[7] FireEye. "M-Trends 2016." February 2016.

AFTER A BREACH

After operations are restored from a breach, one important question company executives should ask themselves is "Could this happen again?" They need to create a framework to identify gaps and vulnerabilities in their systems and decide what and how to improve.

Changes could include hardening firewalls and upgrading security appliances that guard your email, end points or mobile devices. If an intruder gained access to your network by first breaking into a partner's network, that vulnerability must be addressed.

Weaknesses in breach response planning may also be revealed. Examples might include:

- Call center overwhelmed by customer queries, indicating the need for improved logistics and communications
- Tarnished reputation and loss of consumer confidence as a result of negative press and social media commentary, demanding a stronger communications plan
- Recognition of poor security hygiene in the general workforce, necessitating upgraded security awareness and training

Breaches also result in legal complications, such as consumer and shareholder lawsuits, and regulatory investigations. Although organizations can purchase cyber insurance to offset such risks, there is no industry standard or governance for underwriters. Reviewing the fine print falls to your legal department and COO. SAFETY Act certification, carried by several FireEye products, provides a federally-backed opportunity to augment that insurance: liability protection for third party claims when a cyber attack is deemed an "Act of Terrorism" (which is broadly defined).

Increasingly, companies are seeking improved intelligence about threats they face, since their core businesses do not encompass intelligence gathering efforts. They often contract with a service provider that offers vast global resources to identify various potential attackers and the methods they use to attack.

To implement its cyber security framework, your company must adjust budgets as required, and include input from C-level executives on how to meet the needs of each of their departments.

CHAPTER 5

VIGILANCE AS THE NEW NORMAL

For some companies, it takes a breach to come to terms with the reality of constant threat to our cyber landscape. They realize the threat doesn't go away because they survived a single incident. But there's no need to wait for a breach to establish a strong security mindset. It's far better to prepare properly for a breach and then, when necessary, respond smartly and recover quickly when incidents occur.

As the cyber landscape becomes more precarious, it is becoming clear that every C-level executive has a unique and critical role to play. If you take an active role in understanding cyber security risks and collaborating with your peers, you are better positioned to protect your organization. You can also help your company move beyond simple security compliance to true security leadership.

To learn how you can advance your organization's cyber security posture, please visit **www.FireEye.com.**

Disclaimer: The information presented here is not meant to constitute legal advice. Every situation is unique; this guide is not a substitute for experienced legal counsel or cyber security expertise. FireEye strongly recommends consulting legal and security professionals when mapping out a cyber defense strategy and responding to incidents.

For more information, visit:
www.fireeye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@fireeye.com

fireeye.com

FireEye