PROTECTING YOUR DATA, INTELLECTUAL PROPERTY, AND BRAND FROM CYBER ATTACKS:
A Guide for CIOs, CFOs, and CISOs
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Today’s Threat Landscape</td>
<td>4</td>
</tr>
<tr>
<td>The Advanced Persistent Threat Menace</td>
<td>5</td>
</tr>
<tr>
<td>The High Cost of Weak Security</td>
<td>6</td>
</tr>
<tr>
<td>Reputation Damage</td>
<td>7</td>
</tr>
<tr>
<td>The C-Suite Role in Smarter Security</td>
<td>8</td>
</tr>
<tr>
<td>From Point Products to Adaptive Cyber Defenses</td>
<td>9</td>
</tr>
<tr>
<td>Threat Intelligence as a Service</td>
<td>10</td>
</tr>
<tr>
<td>Start from the Top with Adaptive Defense</td>
<td>11</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Keeping up with the volume of network alerts and the new techniques that cyber attackers are constantly developing can be exhausting for security teams. Organizations spend a considerable amount of time and money on cyber security, but the attacks keep coming—and many of them breach networks.

Although cyber defenses are getting stronger, top executives remain under increasing pressure to step up. They are tasked with protecting valuable corporate data such as financial assets, intellectual property, and customer and employee records.

To protect networks and the corporate data traversing them, executives need to obtain advanced intelligence that reveals more about the attackers than what is available from limited point security solutions. They also need to advocate for and deploy adaptive defenses that can react quickly as attackers try different methods to break into their systems.
Today’s Threat Landscape

Cyber criminals attack for a variety of reasons. Greed motivates some to steal credit card and bank account information to obtain cash. In other cases, attackers steal corporate secrets to trade on inside information. Others operate as “hacktivists” by releasing confidential information to embarrass a person or organization, or to make a political point.

Attacker motives vary and so do their methods. Attackers are finding new ways to get into corporate networks, whether via email, web browsers, routers or mobile devices. For example, FireEye recently published research on WITCHCOVEN, a profiling script that cyber attackers use to infiltrate web analytics systems, which collect, analyze and report user and device data from the web.

The APT Menace

Today’s serious cyber threats come from advanced persistent threat (APT) groups. These groups use multiple vectors to try to break into a target network and are unrelenting in their efforts. APT groups usually have either direct or tacit approval from a government.

What makes APT groups and their methods particularly devious is their stealth. Attackers can breach networks, lie low, study how the network operates and then launch attacks on their schedule. According to the M-Trends 2015 cyber security report from Mandiant, a FireEye company, threats of all kinds, including APTs, were present for an average of 205 days on a victim’s network before they were detected. Intruders remained so well hidden that only 31% of victims discovered the intruder on their own. The other 69% learned about the breach from an external party.

Examples of APT groups include APT3, a group with origins in China that FireEye has linked to attacks on companies in aerospace, defense, construction, energy and other high-tech industries. APT28 is another group that steals sensitive political and military intelligence for the Russian government. There are dozens of such APT groups believed to be operating globally. FireEye maintains dossiers that document their activities, their motives and their tactics, which might include spear phishing, social engineering, malware and crimeware.

What these emerging APT threats reveal is that many companies lack the sophisticated and advanced cyber security systems they need to protect themselves. They may think they are protected by widely deployed security technology such as antivirus (AV) software, firewalls and intrusion prevention systems (IPS), but many cyber criminals have learned how to get around those signature-based technologies.

---

3 Ibid.
The High Cost of Weak Security

A cyber security breach can mean big financial losses. Attackers can take money directly from your company, disrupt your operations, damage your brand reputation and put your customers and employees at risk.

In addition to the obvious financial losses from theft and the cost to restore systems, there are many indirect but equally crucial costs. According to the “2015 Cost of Data Breach Study: Global Analysis,” published by Ponemon Institute, the average cost to a company from a breach was $3.8 million, a 15% increase from the prior year. On average, each compromised record costs a target company $154, a 12% increase over the prior year.

The negative impact on your customers and employees can be significant if personally identifiable information (PII) is stolen. You may be liable if they become victims of cyber attacks due to your inadequate security. For example, the records of more than 21 million current or former employees of the U.S. government were put at risk because of a breach at the federal Office of Personnel Management (OPM). Multiple lawsuits have been filed as a result.

Cyber attacks can also hurt your competitive edge. Cyber thieves can steal unreleased intellectual property and learn about company secrets, including business strategies, product launches and merger and acquisition plans.

Meanwhile, many government and industry organizations can impose costly financial penalties for having inadequate security. Security and privacy regulations are enforced by the U.S. Securities and Exchange Commission (SEC), the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS), to name just a few. There are even laws that cover customer notification. Several U.S. states require companies, at their own expense, to notify customers in the event of a breach. The European Union is in the process of rolling out similar rules.

In addition to the cost of acquiring new technology to patch holes in security, credit card issuers may also incur the expense of distributing new credit cards and account numbers to customers. There can also be unforeseen expenses associated with financial audits and possible lawsuits. These all can sap productivity because that time and money cannot be invested in core business objectives.

---

7 Ibid.
Reputation Damage

If you have to notify your customers of a breach, prepare for negative publicity. Major companies in recent years have seen TV news vans pull up at their corporate headquarters as media seek comment on the latest attack. Companies also have to endure negative publicity from social media and even just word-of-mouth. Your company will need to create a public relations campaign across multiple platforms to explain what happened, how you’re addressing the problem and what you’re doing to win back customer confidence. Your reputation and business may suffer if customers no longer feel their credit card accounts and other personal information are secure when they try to do business with you.

The C-Suite Role in Smarter Security

Because cyber threats continue to grow, the top people in an organization have to be more diligent about advocating good cyber security practices. According to the Ponemon Institute, “79% of C-level executives in U.S. and U.K. companies say executive level involvement is necessary to achieving an effective incident response to a data breach.”

While the chief executive officer (CEO) has overall responsibility for maintaining an organization’s cyber security posture, the chief information security officer (CISO)—or the chief information officer (CIO)—is the key executive who manages cyber security.

But all C-level executives have critical roles to play in formulating the company’s cyber security strategy in consultation with their IT department and outside security vendors. The chief financial officer (CFO) needs to protect corporate financial assets and make sure cyber security budgets receive adequate funding. The chief marketing officer (CMO) is a key part of the incident response team in order to implement the company’s communications strategy. Because breaches are increasingly likely to go public—and sometimes must be disclosed—the CMO works with other communications consultants on a communications plan. The chief human resources officer (CHRO) must protect personnel records, which are increasingly subject to privacy laws. Each executive needs to work with their CISO to decide what data is most important to secure, what technology is best for securing it and how best to deploy and manage that security.

In addition to good overall departmental security, executives should also stress good cyber security best practices with their employees. These range from not using “password” as a password to guarding against spear-phishing attacks. Better hygiene is the first line of defense against malicious malware downloads and the loss of PII.

Major companies in recent years have seen TV news vans pull up at their corporate headquarters as media seek comment on the latest attack.

---

7 Ibid.
From Point Products to Adaptive Cyber Defenses

In the wake of an incident, organizations usually conduct an internal review to determine where their security failed and how to improve it. The analysis can identify weaknesses in their network, email systems, computers, mobile devices and procedures. Then, they implement new and smarter cyber security defenses for modern security threats. However, you don’t have to wait for a cyber attack to improve security.

Today, organizations are increasingly considering the FireEye Adaptive Defense approach which analyzes, all IT components as an ecosystem. It uses analytics, threat intelligence and forensics to identify specific risks to your organization and determine how to address those risks.1 Adaptive Defense helps your security evolve. It guides you as you learn and improve to deal with new cyber threats.

The Adaptive Defense approach provides greater protection than point solutions such as AV software or IPS. Point products, often from different vendors, have limited effectiveness because they can only search for security threats with known signatures, and only within a specific vector or device type. They cannot spot zero-day attacks with unknown signatures. With such limited insight, security teams usually end up chasing false or insignificant alerts that prevent them from focusing on genuine threats.

A survey of IT professionals prepared for FireEye by IDC revealed that nearly half of alerts they received turned out to be false positives and that one-third of all alerts were redundant alerts across multiple threat detection platforms. Further, the survey shows that only about half of the redundant alerts received turned out to be an actual malicious event.2 The mission of an Adaptive Defense is to reduce the time wasted chasing redundant or false alerts.

Alert Duplication

- Respondents indicated that nearly half of alerts were false positive and over one-third of alerts were redundant across multiple threat detection platforms.
- Less than 60% of respondents implemented a process to automatically ignore duplicate alerts. This was driven in part by Latin America, which had the highest amount of manual reviews.
- A large number of organizations are manually responding to redundant alerts that are only 50% likely to be an actual malicious event.

Source: IDC Survey, sponsored by FireEye, Advanced Threat Readiness Assessment, September 2014; n=505

Threat Intelligence as a Service

Superior threat intelligence is a critical element of Adaptive Defense. It helps make sense of the threat landscape beyond your own network perimeter. You should look for intelligence services that provide broader insight into threat actor tools, techniques and procedures (TTPs). These services provide scarce and valuable expertise and help you prioritize critical security activities.

Threat intelligence can uncover major cyber plots. For example, cyber criminals used subterfuge to connect with rebel forces challenging the rule of Syrian President Bashar al-Assad. The attackers downloaded malware onto the rebels’ computers and mobile devices and stole tactical military information about the rebels’ plans. This intel was not gleaned by simply monitoring network traffic; a network of human intelligence sources was needed to explain what was happening.

As cyber attacks grow in number, size and sophistication, it’s easy to become overwhelmed. Appliances that guard your network, endpoints and email systems can’t always keep up with the volume of traffic they encounter. This type of environment helps make the case for engaging a security service provider.

In addition, some organizations cannot afford to hire more qualified experts to staff their security teams in a tight labor market. The ISACA 2015 Cybersecurity Global Status Report explains the challenge: “86 percent of companies surveyed said that they see a global cyber security skills gap. Also, 92 percent of those planning to hire more cyber security professionals this year say they expect to have difficulty finding a skilled candidate.”

Given these constraints, organizations that recognize the need to enhance cyber security are increasingly embracing the service model, contracting with an outside firm for advanced intelligence and defense capabilities. This way, the service provider takes on the capital and staffing expense of building the intelligence capability.

---

92 percent of those planning to hire more cyber security professionals this year say they expect to have difficulty finding a skilled candidate.

---

Start From the Top With Adaptive Defense

As an executive, you can exhaust yourself trying to protect your networks and data from multiple cyber threat groups. The attackers often have diverse motives and possess considerable resources, often from sponsoring nation states. Traditional tools deployed to protect your networks are easily thwarted by advanced threat actors. You can also be distracted by false and redundant alerts that waste time and money without delivering actionable results. Meanwhile, the consequences of a network breach are considerable. Beyond just the loss of data, you risk damage to your company’s business model, its intellectual property and its reputation. To help you keep pace with modern cyber threats, the industry-leading FireEye Adaptive Defense approach offers sophisticated intelligence capabilities and a security-as-a-service model to protect you without prohibitive capital investments.

For additional executive guidance on modern cyber threats and defenses, please visit www.fireeye.com.

FireEye Adaptive Defense offers sophisticated intelligence capabilities and a security-as-a-service model to protect you without prohibitive capital investments.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you’ll detect attacks as they happen. You’ll understand the risk these attacks pose to your most valued assets. And you’ll have the resources to quickly respond and resolve security incidents. FireEye has over 3,100 customers across 67 countries, including over 200 of the Fortune 500.
To learn more about FireEye Adaptive Defense, visit:
www.fireeye.com