THE CYBER RISK PLAYBOOK

WHAT BOARDS OF DIRECTORS AND EXECUTIVES SHOULD KNOW ABOUT CYBER RISK

JULY 2016

FireEye

CHAPTER 1

INTRODUCTION

The cyber threat landscape has changed. Attackers are now targeting more and different types of data to extort or otherwise harm your business. Although commodity malware and other traditional attacks still exist, threat actors now can expand their reach and skillsets through underground markets. They can hire additional expertise and buy additional exploits that exceed their own capabilities. Business leaders must take note of the changing risk and keep their breach response plans current.

More importantly, as cyber attacks become more frequent and more sophisticated, businesses must take cyber risk seriously at the highest organizational levels. Responsibility can no longer be relegated to the IT department alone. Data breach preparedness must start at the top.

This playbook provides boards of directors and executives with cyber risk management best practices to provoke discussion and encourage planning. Our recommendations draw on extensive experience preventing, investigating and resolving cyber attacks for companies across the globe.

Our goal is to help your organization protect itself from reputation damage, litigation and liabilities that can occur following a breach or other cyber crisis events.

CHAPTER 2

THE REALITY OF CYBER RISK

Most organizations are aware of and have plans to address their financial, legal and insurance risks. But what about the cyber risks?

We live in an era where a month doesn't go by without another major data breach in the news. Yet these high-profile cyber attacks represent only publically reported incidents. Many breaches never make it into the media. Every company today has a global exposure to such risks. And if cyber risk isn't a board-level discussion now, it will be when your company experiences a significant breach.

Figure 1. What are cyber attackers after?

Attackers have many different motives and goals, any of which can hurt your business and have far-reaching impact on stock price, future merger and acquisition deals, brand reputation and even market viability.

POLITICAL OR MILITARY ESPIONAGE

Targets military research and development organizations, government agencies and think tanks to compromise their operations or steal information.

COMMERCIAL ESPIONAGE

Targets private and public companies to steal or damage confidential or proprietary information.

DISRUPTION

Targets networks or systems to vandalize them or delete or corrupt data.

CYBER CRIME

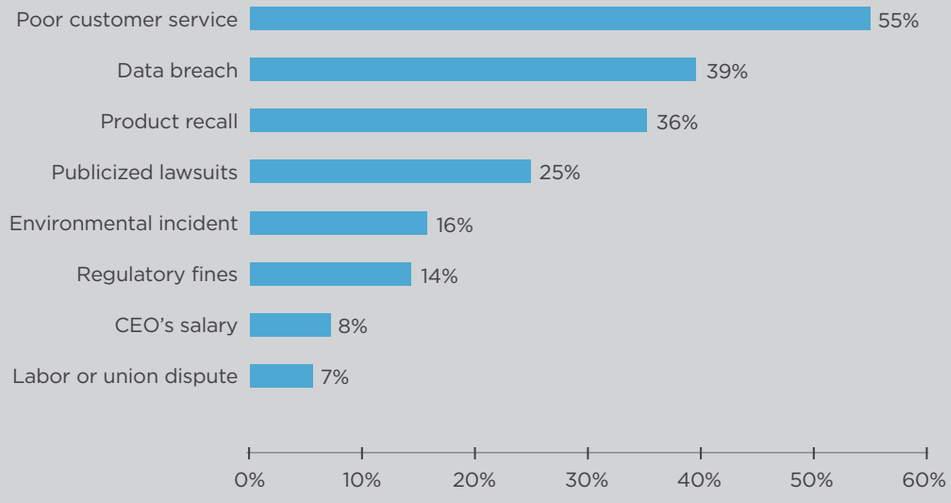
Targets networks and systems to steal data that can be directly or indirectly used for financial gain.

Here are several ways cyber attackers can harm your organization:

- **Exposure.** Corporate secrets, customer and employee personal information and other proprietary data can be exposed to competitors, the black market or the general public.
- **Corruption or destruction of data.** Attackers can enter your environment to delete, change or destroy valuable corporate information assets.
- **Disruption of operations.** Remediation after an attack may require you to take servers and systems offline to ensure you've identified and mitigated the full scope of the damage.
- **Extortion.** By using ransomware or destructive malware, cyber attackers can encrypt or destroy data, and in some cases threaten exposure of sensitive communications and information unless you pay a substantial fee. Rebuilding an entire network infrastructure that was attacked by destructive malware could even affect your ability to remain in business.

According to a PricewaterhouseCoopers 2016 report on cyber risk, the number of detected cyber attacks skyrocketed in 2015 — up 36% from 2014. They are expected rise even further in subsequent years, with businesses around the world already enduring more than 117,000 attacks each day.[1] Computer crime emerged for the first time as a top 10 risk in AON's 2015 Global Risk Survey.[2] And although getting known for poor customer service is still considered the most serious threat to a business, data breaches have risen to second place, with 39% of companies saying it would have the greatest impact on their reputation (Fig. 2.)[3]

Figure 2. Issues companies think will impact their reputation the most.



Source: Advisen. "Fifth Annual Report on Risk." 2015.

[1] PricewaterhouseCoopers. "The Global State of Information Security Survey." 2016.
[2] AON. "Global Risk Survey." 2015.
[3] Advisen. "Fifth Annual Report on Risk." 2015.

What is the financial cost of cyber attacks?

Cyber risk evolves quickly and is difficult to predict. Yet the damage from failing to take it seriously can be immense. A Washington think tank, the Center for Strategic and International Studies, claims that the annual cost of cyber crime and economic espionage to the world economy runs as high as $445 billion — or almost 1% of global income. This doesn't include the intangible damage to organizations, such as damage to brand and reputation.[4]

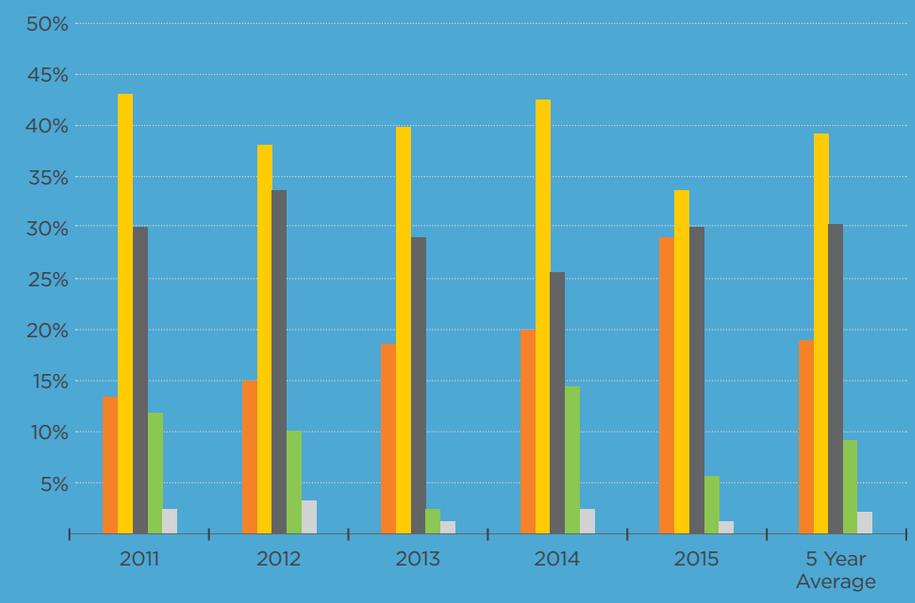
The Ponemon Institute found that the average cost of a breach is rising, reaching $7.7 million in 2015.[5] Business disruption accounts for 39% of total costs, which include expenses related to business process failures and lost employee productivity. Detection is the most costly activity. Detection and recovery costs combined account for 53% of the total cost, with productivity loss and direct labor representing the majority of these costs.[6]

Despite this, Advisen's Fifth Annual Report on Risk 2015 found that the number of executives who ranked cyber risk as "serious" actually dropped — from 42% in 2014 to just 34% in 2015, with more respondents ranking cyber risk as "moderate" or "mild." (Fig. 3.)[7]

The good news is that more businesses see cyber security as an organization-wide challenge rather than just something to be dealt with by the IT department. Greater awareness at the executive and board levels has led many organizations to hire a chief information officer (CIO) or chief information security officer (CISO) to head their cyber risk management efforts.

But of the 81% of respondents who say their company has an incident response plan, only 34% say these plans are either "effective" or "very effective." This is a slight increase from 30% in 2014. Thus, major gaps remain in how organizations prepare for data breaches or other cyber security crises.[8]

Figure 3. How companies rate cyber security risks.



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

4 Center for Strategic and International Studies. "The Economic Impact Of Cybercrime And Cyber Espionage." 2013.

5 Ponemon Institute. "Cost of Cyber Crime." 2015.

6 Ibid.

7 Advisen. "Fifth Annual Report on Risk." 2015

8 Ponemon Institute. "Third Annual Study: Is Your Company Ready for a Big Data Breach?" October 2015.

CHAPTER 3

BOARD AND EXECUTIVE RESPONSIBILITIES

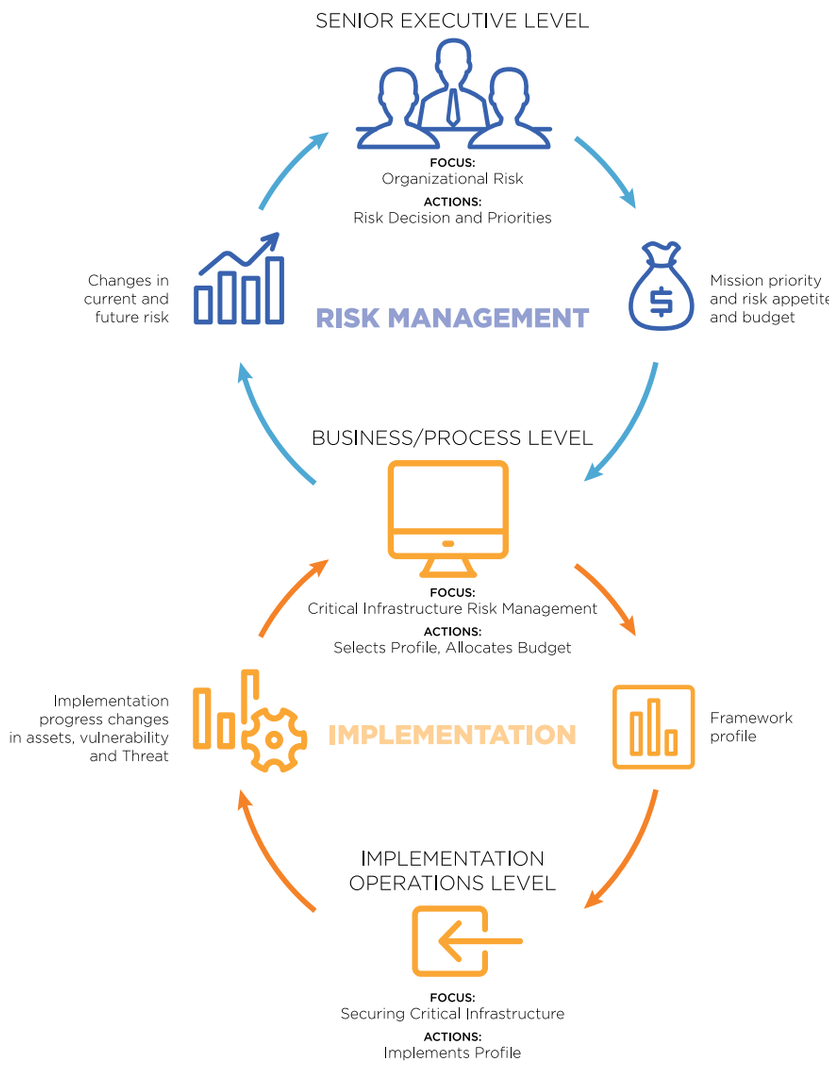
Boards of directors, chairmen and CEOs have become more involved and informed in the past 12 months about their companies' plans to deal with a possible data breach. In 2014, only 29% of respondents said their senior leaders were involved in data breach preparedness. This year, possibly due to the publicity over recent breaches, 39% of respondents say their boards involved in data breach preparedness.[9]

We also saw a significant increase — from 45% to 54% — of respondents who report their boards and C-suite participate in high-level reviews of the data breach response plans.[10]

Although this improvement is encouraging, boards need to take steps to ensure their participation is productive:

- **Include key stakeholders from the company in cyber risk decisions.** This should include business leaders, legal, corporate communications, the CIO and the CISO. (Fig. 4.)

Figure 4. The board must involve stakeholders from across the company



[9] Ibid.

[10] Ibid.

THE LEADERSHIP ROLE IN CYBER SECURITY

As part of cyber risk management, board members and executives should:

- Conduct a cyber risk assessment.
- Stress the importance of the assessment to facilitate timely responses from people throughout organization.
- Align the cyber security preparedness level to match the board's risk appetite.
- Review, approve and support plans to address risk management and control weaknesses.
- Analyze and present results for executive oversight, including key stakeholders and either the board or an appropriate board committee.

- **Fully understand the legal implication of cyber risks.** In addition to fees assessed by government or regulatory agencies, there has been a rise in shareholder litigation, typically consumer class action suits and shareholder derivative litigation. Claims against boards and even individual board members include breach of fiduciary duty, corporate waste and mismanagement, with the key allegation being that directors or officers did not take sufficient steps to prevent a cyber attack that resulted in monetary or reputational harm to the company.[11] This means you must be prepared to show that you took reasonable cyber security measures (see "Demonstrate That You Took Reasonable Cyber Security Measures," p. 9).
- **Get adequate access to cyber security expertise.** This helps board members and executives understand the overall risk landscape, the technology solutions available and best practices for responding to a breach. If this expertise is not available in house, this expertise must be acquired from a third party.
- **Discuss cyber risk management regularly on the board meeting agenda.** This ensures that management establishes an enterprise-wide risk management framework with sufficient staffing and budget. To be effective, a risk-management framework should be integrated with the various layers of service management such as change management, problem management and incident management.

[11] The Business Litigation Reporter. "Breaches in the Boardroom: What Directors and Officers Can Do to Reduce the Risk of Personal Liability for Data Security Breaches." February 6, 2015.

[12] Ibid.

DEMONSTRATE THAT YOU TOOK REASONABLE CYBER SECURITY MEASURES[12]

Executives and the board must demonstrate that they took reasonable steps to fulfill their fiduciary duties to shareholders for cyber security. Failure to do the following could be considered "unreasonable:"

- Remedy known security vulnerabilities such as allowing insecure server/network connections
- Employ commonly used methods to require user IDs and passwords that are difficult for hackers to guess
- Adequately inventory computers to manage network devices
- Employ reasonable measures to detect and prevent unauthorized access or to conduct security investigations
- Follow proper incident response procedures such as monitoring computer networks for malware used in a previous intrusion
- Adequately restrict third-party vendor access
- Share threat information or act on shared information

CHAPTER 4

A RISK MANAGEMENT FRAMEWORK

WHAT IS RISK? RISK CAN BE DEFINED AS:

"A probability of threat or damage, injury liability, loss or any other negative occurrence that is caused by external or internal vulnerabilities, and which may be avoided through preemptive action."[13]

We have a formula for the cost of risk:

Cost of Risk = (Threat x Vulnerability) x Impact

What do these terms mean?

- **Risk:** Annual loss expectancy in dollars.
- **Threat:** Anticipated potential attacks (based on threat intelligence and past experience).
- **Vulnerability:** Average exposure (0% to 100%) across your infrastructure.
- **Impact:** Cost per event.

The impact can be broken down further into:

- **Actual losses:** Lost revenue, lost time, lost customer base, lost production output, and other considerations.
- **Recovery costs:** What it costs to identify, detect, investigate, contain and eradicate the threat.
- **Legal costs:** Regulatory fines and shareholder or customer lawsuits.
- **Reputational and brand damage:** Lost competitive advantage, lost value to brand.

[13] Businessdictionary.com

A Five-Step Risk Framework

STEP 1:
Assess your security program

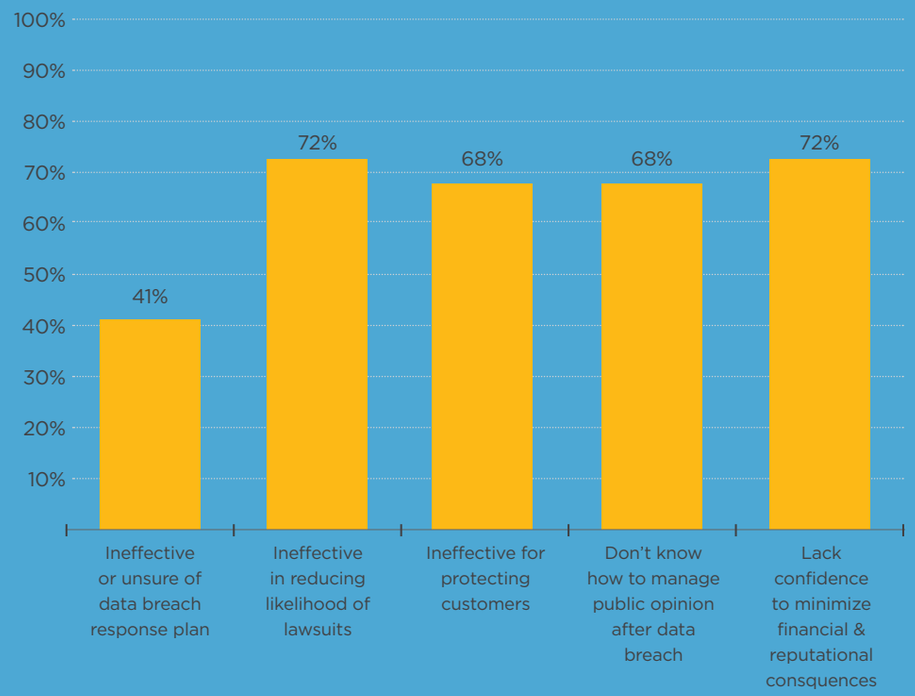
To understand how the organization discovers, manages and mitigates risk, executive and board members must take deep dives into what technology platforms are in place to deter, prevent, detect and respond to breaches, as well as what mechanisms — typically insurance — are in place to transfer risk.

Despite increased security investments and incident response planning, when asked about the preparedness of their organizations, most senior executives are not confident in how they would handle a real-life issue (Fig. 5.)[14]

An essential point: the board needs to understand who owns cyber risk. The good news is that when asked, "Is there a key executive with oversight responsibility or whose main focus is cyber security?" 74% of businesses said, "Yes." The bad news is that not enough businesses understand that cyber risk management must involve skilled personnel from the entire organization. Only 57% said they had a multi-department information security risk management team.[15]

To fully understand your current state of cyber risk, hire an independent expert third party to validate the security technologies, people and processes in place by conducting a cyber risk assessment.

Figure 5. Management not confident about breach preparedness.



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

[14] Ponemon.

[15] Advisen. "Fifth Annual Report on Risk." 2015

STEP 2:

Understand your current threats

Does your organization have the capability and resources to understand the current, known threats that your company faces?

For example, some of the biggest headlines have involved breaches in which the attacker entered a target company via a smaller and relatively unprotected third-party partner. A full 25% of companies don't monitor the incident response plans of their partners, even though 44% of the same businesses rank third-party access to data as one of the biggest barriers to their ability to respond effectively to a data breach.[16]

Understanding the current threat landscape requires intelligence — up-to-the-minute intelligence from a reliable source. You may consider joining one of many organizations that share information among industry peers or within a particular geographic area. Expert third-party incident response firms also have large, ever-evolving intelligence databases that they share with their customers in real time. Gleaning intelligence and transforming it to proactive defense is key to protecting your organization.

STEP 3:

Understand evolving threats

Even as companies attempt to improve their cyber defenses, the cyber risk landscape is evolving. Traditional data assets such as customer payment records, bank account numbers and credit card numbers have flooded the black market in recent years, lowering their commercial value. As businesses and consumers lock their credit records and become savvier about online attempts to defraud them, it's more difficult for cyber criminals to get quick financial gain by accessing accounts. Corporate extortion is becoming a growing threat, with 38% of businesses saying they have already been targeted by cyber extortionists.[17] (See "Attacks are Cheap," p. 13.)

Cyber security intelligence — the kind of intelligence you won't get from reading general business or trade press, or from talking to peer organizations — is critical to understanding evolving threats. For real cyber intelligence, you need to turn to people who are on the front lines of the war against cyber criminals.

ATTACKS ARE CHEAP

Prices of traditional stolen data assets have declined precipitously on the black market, leading cyber attackers to seek other ways to monetize criminal activities, such as extortion.[18]

- Stolen email account: **$0.50**
- Scans of real passports: **$1**
- Custom malware: **$12**
- 1,000 followers on social networks: **$1**
- Stolen cloud account: **$5**
- Sending spam to 1 million verified email addresses: **$70**
- Credit card data: **$0.10**
- A drive-by download web toolkit: **$100** (rented for a week)
- Online banking malware: **$150** (leased for six months)
- Distributed denial-of-service attacks: **$10** per day

[16] Ponemon Institute. "The Cost of Data Breach." 2015.

[17] Negotiating with Cybercriminals: 30% of Security Professionals Say They Would Pay for the Return of Their Data," ThreatTrack, March 2015.

[18] Symantec. "Underground Black Market: Thriving Trade In Stolen Data, Malware, And Attack Services." November 2015.

STEP 4:
Assess your risk

Your organization should have a data classification policy to categorize and inventory all high-value data assets and understand where they reside and how they traverse the network. The network architecture should be segmented to protect those high value assets with increased monitoring and defense mechanisms. Conducting this evaluation provides transparency to key decision makers on how effective the existing protections are, and where there is unacceptable risk.

The median number of days an organization was compromised in 2015 before the organization discovered or was notified of a breach was 146.[19] Although this was 50 days fewer than the previous year, 146 days is still too long.

A case in point: Mandiant red teams simulate attacks on companies to determine the strength of their cyber defenses. They can typically obtain access to domain administrator credentials within just three days of gaining initial access to an environment.[20] That would theoretically leave more than four months for an attacker to enjoy free reign inside the environment. A lot of damage could be inflicted in that time.

STEP 5:
Decide how to manage the risk

Once your organization has completed its risk assessment, it can make informed risk decisions. Here are four ways to manage risk:

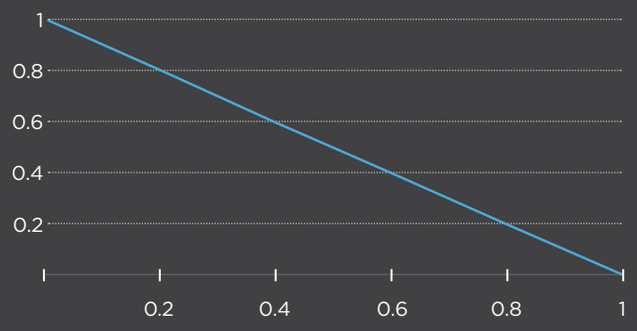
- **Avoid.** Some security technologies will deter cyber criminals from trying the easiest and most obvious strategies for infiltrating your environment, and can protect you from such things as phishing and malware attacks. These include firewalls, intrusion prevention systems, spam filters, anti-malware and other basic security solutions.
- **Mitigate.** Today, most security experts say that it's essential to prepare for a breach — that sooner or later, an attacker will be successfully compromise your systems. You need technology, people and processes to proactively hunt, detect, investigate and remediate to accurately identify the scope of the breach and mitigate the damage. If your staffing levels are not adequate to sustain a long-term investigation and remediation process, consider contracting with a company that specializes in breach remediation and keep them on retainer until their expertise is required. Figure 6 shows how aggressive you may choose to be when investing in security solutions to mitigate risk for your business.
- **Accept.** Some risks you may simply decide to accept. For example, some risks may be deemed too remote or otherwise not important enough to attempt to mitigate.
- **Transfer.** Finally, you may want to transfer a certain amount of risk to a third party—namely, an insurance company. In the event of a breach, you won't bear the full financial burden. Not surprisingly, demand for cyber insurance has grown considerably in recent years. Last year, the insurance industry reaped $2.5 billion in premiums on policies to protect companies from losses resulting from attacks. That was up from around $2 billion a year before, and less than $1 billion two years before that.[21]

[19] Mandiant, a FireEye company. "MTrends 2016." February 2016.

[20] Ibid.

[21] Stephen Gandel (Fortune). "Lloyd's CEO: Cyber attacks cost companies $400 billion every year." January 23, 2015.

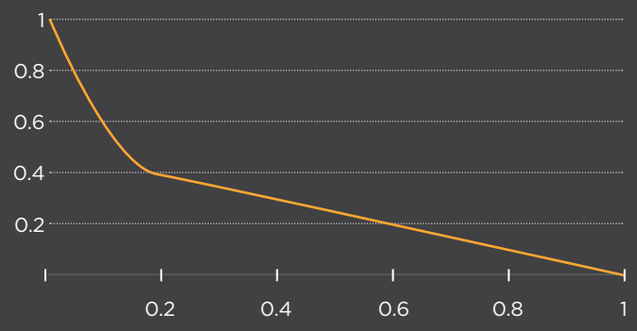
Figure 6. Three possible models for risk mitigation.



LINEAR RISK MODEL

Linear Risk Mitigation

- Risks are reduced in direct proportion to deployment of solutions/mitigations.
- Rapid deployment and full coverage are both critical to effective security control.



DAMPENED RISK MODEL

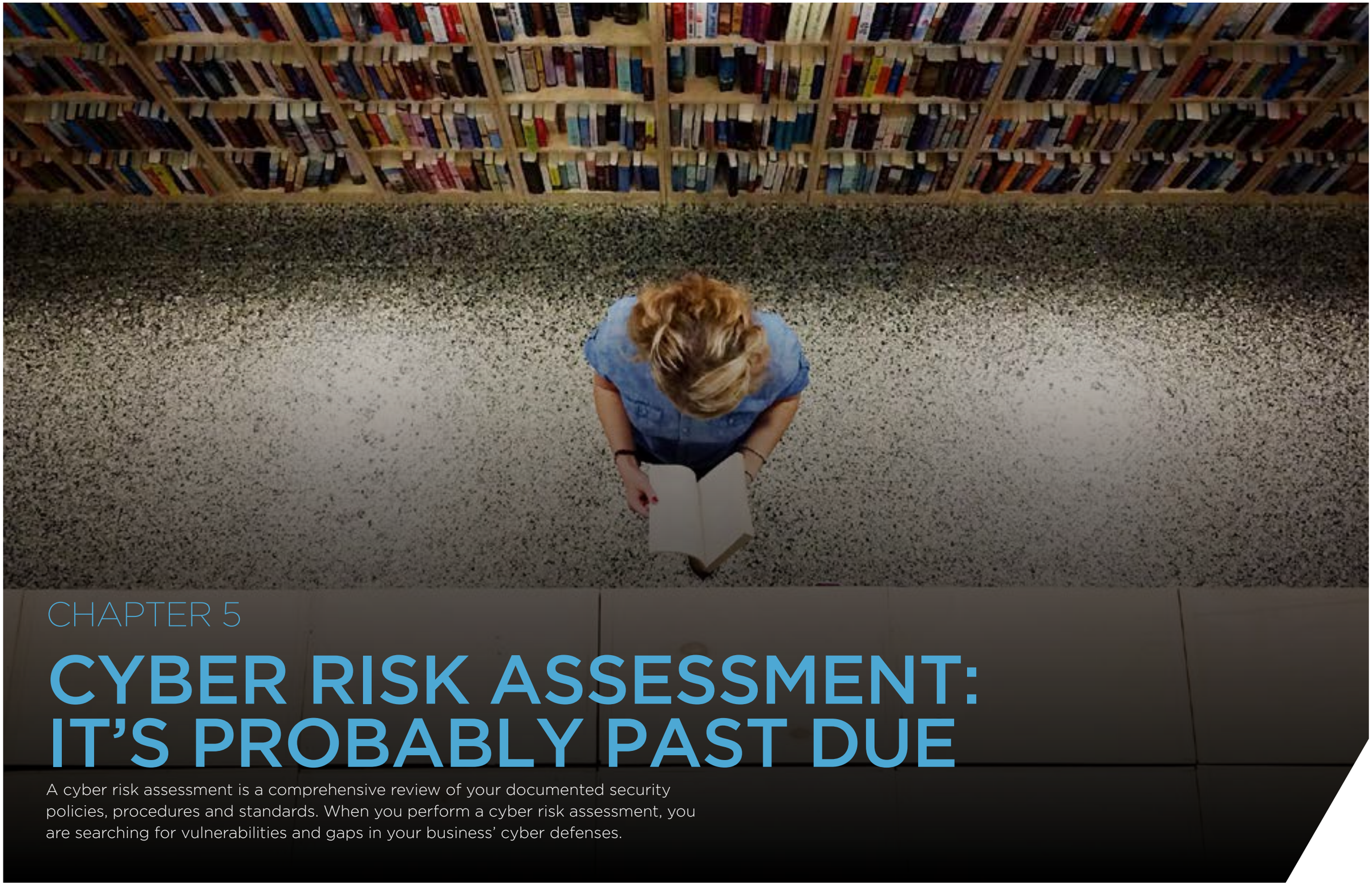
Dampened Risk Mitigation

- Risks are reduced rapidly upon initial deployment with additional risk reduction tapering.
- Rapid time to value. Focus on areas of easy adoption.

AMPLIFIED RISK MODEL

Amplified Risk Mitigation

- Risks are reduced exponentially when a critical threshold of the solution deployment is reached.
- Longer time to value. Must focus on wide-scale coverage and adoption.



CHAPTER 5

CYBER RISK ASSESSMENT: IT'S PROBABLY PAST DUE

A cyber risk assessment is a comprehensive review of your documented security policies, procedures and standards. When you perform a cyber risk assessment, you are searching for vulnerabilities and gaps in your business' cyber defenses.

After taking into account lessons learned from previous incidents at your company as well as known threats to peer companies, a cyber risk assessment will focus specifically on the cyber threats facing your business. It will involve interviews with key personnel, including those with cyber risk management, privacy, procurement and executive responsibilities.

Goals of a cyber security risk assessment

Your cyber risk goals must align with your business goals. Everything from deciding what will be protected to your risk tolerance level must be considered within a business context. From there, you can determine your target state of cyber preparedness.

In many cases, a cyber security risk assessment will compare your program to proven, cyber security frameworks and models such as the National Institute of Standards and Technology (NIST) Cyber Security Framework. This includes evaluating against industry best practices and regulations.

BENEFITS OF A CYBER RISK ASSESSMENT

A cyber risk assessment will also help you:

- Measure the maturity and effectiveness of existing cyber security programs
- Identify security gaps
- Determine short-term, long-term and ongoing cyber security priorities
- Identify investment priorities
- Develop evidence of "reasonable" security measures, including purchasing insurance to transfer risk

10 important questions can be answered by a cyber risk assessment.

Q1:

Who is in charge of your cyber security?

Multiple internal stakeholders often share core cyber responsibilities. Are they integrated? Are there gaps?

Q2:

Does everyone know his or her role?

A clear chain-of-command and established roles are critical to an effective cyber security program. Does the left hand know what the right hand is doing?

Q3:

Who conducts risks analysis, when and with what assets or third parties?

It is vital that your company has experts examining its cyber risks and threats and that such analyses are conducted regularly.

Q4:

Are you keeping abreast of the latest threat intelligence?

Cyber threats and vulnerabilities change on a daily basis, and you are expected to monitor both.

Q5:

What's your process for integrating risk analyses, threat assessments and results?

All relevant information must be continually plugged into your cyber security programs.

Q6:

Are you partnering with law enforcement and industry peers?

You can share key information and build relationships with many groups to establish a smooth network in the event of an attack.

Q7:

Do you have response teams inside and outside the company?

Outside vendors often provide fresh eyes and additional, advanced technical support.

Q8:

Are you assuming a breach or other successful attack is inevitable?

If no, why not?
Not acknowledging this inevitability is a recipe for failure.

Q9:

Are you adequately managing third-party risks?

Many cyber attacks originate from third parties, so vendors, contractors and consultants need to be considered in any cyber security plan.

Q10:

What are you doing to manage and minimize your legal risks and exposures?

Many significant cyber security costs result from post-event investigations and litigation.

CHAPTER 6

AFTER THE CYBER RISK ASSESSMENT

After the assessment, executives and the board must take several actions.

- **Determine the risk appetite of your organization.**

  How risk-averse are you? How much financial risk can you bear? Ultimately, this is a decision only the board can make.

- **Form a crisis or core management team.**

  This team must be ready to respond to any incident at the highest levels when you are alerted to a valid and significant attack in progress. The team's activities may include communications plans, PR engagements and contracting outside legal advice.

- **Develop a crisis-management communication plan.**

  Most breaches today become public within a matter of hours. How will you communicate your situation to the world?

- **Create incident response playbooks.**

  These should come with scripts and key decision points, roles, responsibilities, and decision-making authority levels for the C-suite in additional to the traditional technology-centric ones.

- **Develop relationships with law enforcement.**

  A high percentage of breaches are discovered by law enforcement.

- **Develop evidence of "reasonable" security measures.**

  Be prepared for the legal liabilities that will follow any breach.

- **Create a methodology to handle changing risk due to business changes.**

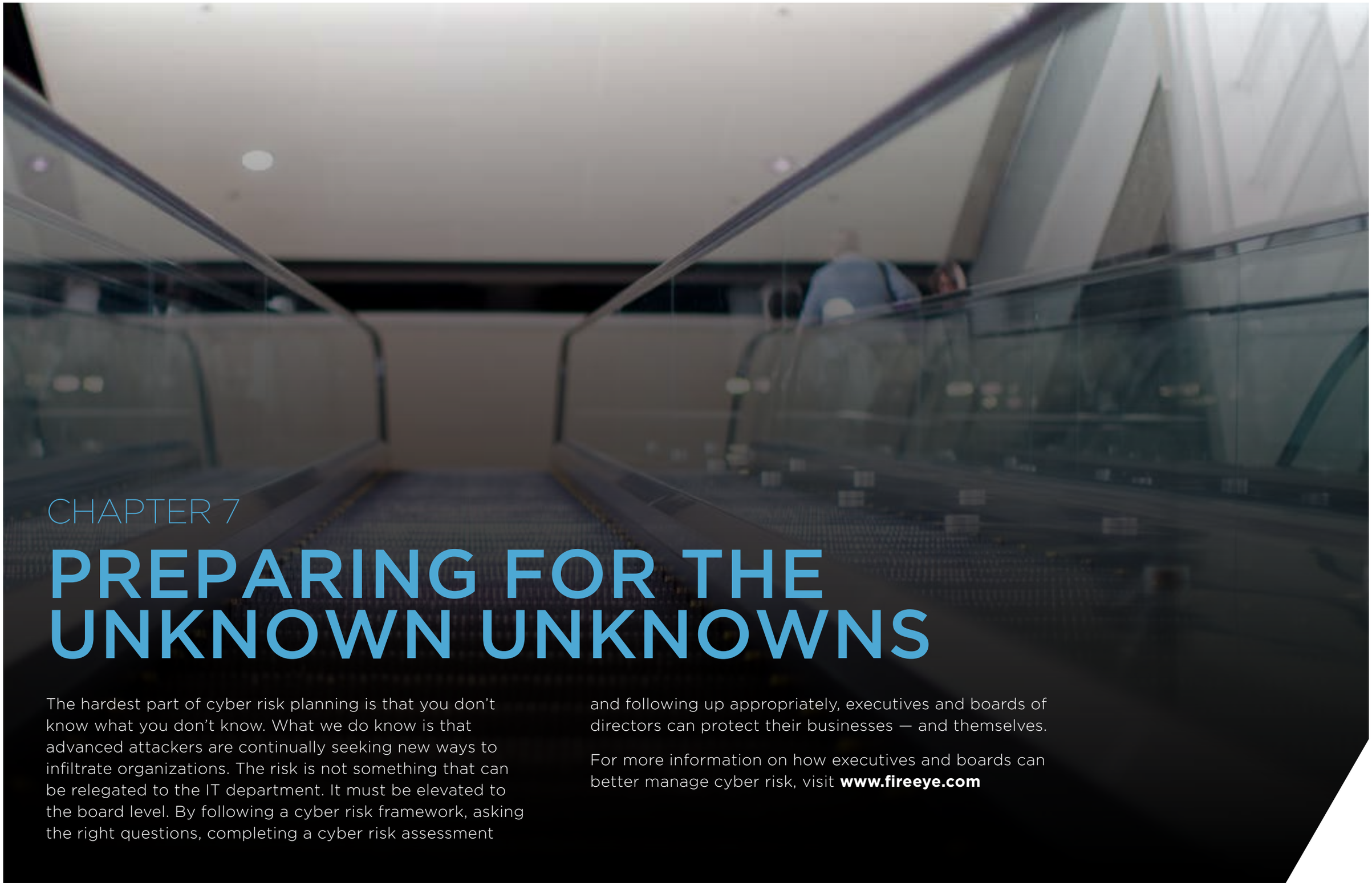
  What happens when you create a mobile app for customers? Move your data center off site? You have to have a process for assessing and mitigating your risk as your business evolves.

- **Conduct cyber due diligence during mergers and acquisitions to minimize risk.**

  This usually isn't done, but it's essential part of understanding the risks of a particular deal.

- **Stay informed of legal decisions regarding cyber security.**

  This is still an emerging area of law, so rules and regulations do change frequently.



CHAPTER 7

PREPARING FOR THE UNKNOWN UNKNOWNS

The hardest part of cyber risk planning is that you don't know what you don't know. What we do know is that advanced attackers are continually seeking new ways to infiltrate organizations. The risk is not something that can be relegated to the IT department. It must be elevated to the board level. By following a cyber risk framework, asking the right questions, completing a cyber risk assessment and following up appropriately, executives and boards of directors can protect their businesses — and themselves.

For more information on how executives and boards can better manage cyber risk, visit **www.fireeye.com**

For more information on how to manage your security risks, 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