THE COMPLETE GUIDE TO

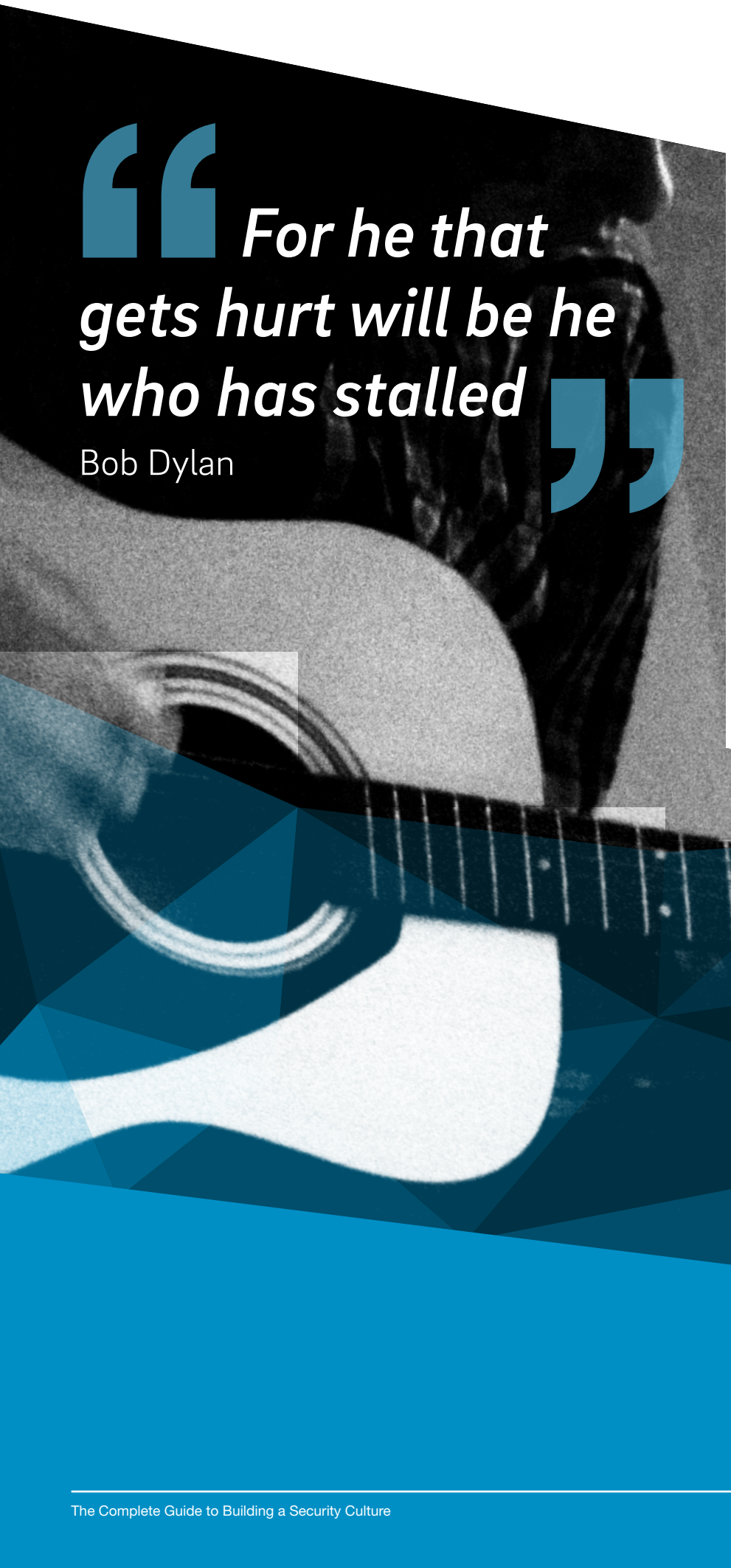
BUILDING A SECURITY CULTURE

Trustwave®

Table of Contents

Introduction

Why Should You Read This Guide?



BOB DYLAN WAS THE VOICE OF A GENERATION, but he wasn't referring to the digital age when he wrote the lyrics to his iconic "The Times They Are A-Changin'" more than five decades ago. But he might as well have been.

IT is driving fundamental changes in the way organizations like yours operate, compete, and engage with customers and partners. The web, cloud services, mobile devices and Internet of Things (IoT) technologies have given rise to wonderful opportunities for businesses to personalize the customer experience, offer innovative delivery models, and to improve productivity and operational efficiencies.

Unfortunately, the same technologies are also creating new opportunities for cybercriminals to attack and disrupt your business, and to steal data from it.

New approaches are required to navigate these challenges. Information security can no longer be just a tactical loss-avoidance function. It must be about enabling business objectives and strategies, and keeping cyber risk at manageable levels, while also dealing with the realities of a severe and deepening skills shortage.

Never before has security culture mattered so much. Silos are dead. The security attitudes, values and practices of every employee across your organization - whether you're a 20-person startup or a 50,000-person Fortune 500 - will be the ultimate definer of the success of your security program.

We have prepared this e-book as a definitive way for you to identify the security challenges you must confront and the reasons why you need to engage with colleagues across your enterprise - and partners away from it - to help mitigate these challenges.

Our hope is that when you're done reading, you've learned three big things:

1. How to build two-way, lasting relationships with the rest of your organization and help grow the business.
2. How to transform security into an instinctual, reflexive practice for all of your employees, and
3. How external allies can help amplify and augment your internal security culture.

Chapter 1

The Case For Change

CLOUD, MOBILE, IOT AND OTHER DIGITAL TECHNOLOGIES CAN HELP TRANSFORM YOUR BUSINESS. But like the tornado that transported Dorothy to the Land of Oz, they can also displace you into a whole new world of unpleasant surprises. Dealing with the risks posed by technology progression requires a fundamentally new understanding of your security needs and how to go about addressing them. Here's why:

01

THE EVER-EXPANDING ATTACK SURFACE

The more ways your organization uses digital technologies to remodel business processes, operations and customer engagement, the more you potentially expand your attack surface and exposure to risk.

Consider the use of cloud-based services such as those commonly used by your employees for collaboration, file synchronization and sharing, data storage, development, and content sharing. Such services can improve productivity by allowing your employees to more easily store, share and collaborate with enterprise data outside the firewall. But allowing workers to use unsecured, unapproved and consumer-grade services can expose critical business data to theft, accidental exposure and misuse.

FACT: *The average enterprise now uses more than 1,425 cloud services. The mostly commonly used cloud services are collaboration tools, followed by file-sharing services. Without a way to discover and monitor cloud services, they pose a huge data security and privacy risk to your organization.*

> ***"Toto, I've a feeling we're not in Kansas anymore."***
>
> Dorothy – "The Wizard of Oz"

Laptops, smartphones and tablet computers, meanwhile, can drive multiple business gains and enable better decision-making in the field by giving users a way to access their enterprise workspace from anywhere at any time. But such gains can quickly be eroded if you don't have measures for securely enrolling, monitoring and managing mobile devices that have access to enterprise data and services.

DID YOU KNOW? *More than six million records containing sensitive data were compromised in 2016 from breaches that resulted from improperly secured mobile devices, including those that did not have basic protections such as encryption.*[1]

The increasing reliance on digital technologies expands your attack surface in other ways. Linking your network with those of suppliers and business partners makes it easier to work with them, but also gives attackers more avenues to pervade your network. Breaches originating at third-parties – which can include point-of-sale vendors – are up 22 percent since 2015.[2] Vendor risk reviews and audits are a baseline tool to measure the security practices of your partners. You can take things up a notch by seeing if they would agree to a penetration test.

Social media channels are optimal for listening to your customers and understanding their needs. They also make it easier for attackers to pull off social engineering scams, conduct reconnaissance on targets and hijack brands.[3] Your marketing and customer support teams should be aware that what they share with the outside world could come back to haunt them.

FACT: *Some of the biggest breaches in recent years resulted from third-party security failures.*

1. https://www.privacyrights.org/data-breaches?title=&breach_type%5B%5D=265&taxonomy_vocabulary_11_tid%5B%5D=2257
2. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
3. http://www.darkreading.com/attacks-breaches/why-social-media-sites-are-the-new-cyber-weapons-of-choice/a/d-id/1326802

02

DATA BREACHES, DATA BREACHES, DATA BREACHES

Traditional network defenses are no longer enough to stop intrusions, compromises and data breaches. Threat actors and the malware they use have become much more sophisticated. Many attacks these days are highly targeted and carried out by well-resourced criminal gangs and nation state-sponsored actors with specific agendas. The result is more breaches than ever before.

FACT: *In 2016, the Identity Theft Resource Center counted a record 1,093 data breaches, or about 40% more than the number of disclosed breaches in 2015.*[4]

The average direct and indirect costs of breach incidents to organizations continue to increase. So too have the legal, brand and shareholder value consequences of data breaches. In 2016, the average cost of a data breach was $4 million, compared to around $3.8 million in 2013.[5] Losses included both the direct costs associated with a breach and the somewhat less tangible costs associated with customer churn and brand damage.

Expenditures for companies that sustain major data breaches can be much higher. For small companies the threat is existential.

FACT: *Sixty percent of small businesses that bear a cyberattack go out of business in six months.*[6]

Customer data theft ranks as the most worrying consequence of a data breach for most organizations.[7] But intruders have other motives as well. Intellectual property theft is a major and growing concern, especially in sectors that rely on trade secrets, such as technology, manufacturing and government. So too is cyber extortion and ransomware attacks, where threat actors encrypt sensitive data and demand a fee for decrypting it.

BELIEVE IT: *Ransomware attacks worldwide grew a staggering 6,000% in 2016.*[8] *Victims included individuals and organizations of all sizes.*

Consumers and government regulators want more accountability from businesses for security failures. Laws are in place or are being developed in several countries, including the United States, that hold chief executives and board members directly responsible for their organization's cybersecurity.[9]

4. http://www.idtheftcenter.org/2016databreaches.html
5. http://fortune.com/2016/06/15/data-breach-cost-study-ibm/
6. http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/
7. https://www.trustwave.com/Resources/Trustwave-Blog/Introducing-the-2017-Security-Pressures-Report-from-Trustwave/
8. http://www.cnbc.com/2016/12/13/ransomware-spiked-6000-in-2016-and-most-victims-paid-the-hackers-ibm-finds.html
9. https://www.congress.gov/bill/115th-congress/senate-bill/536/text?q=%7B%22search%22%3A%5B%22Cybersecurity+Disclosure+Act+of+2017%22%5D%7D&r=1

3

RESOURCE SHORTAGES

If your organization is like a majority of businesses, you are severely short-staffed on the security front. Put simply, there are far too many threats and far too few skilled professionals to help address those threats.[10] The resource crisis, combined with the worsening threat landscape, has left many organizations dangerously vulnerable, and no amount of throwing technology at the problem can alleviate the situation, especially if they lack the internal resources to adopt and deploy it.

The shortage is especially critical in areas such as security analytics, penetration testing, threat detection and response, and incident readiness and response.

IN AN OSTERMAN RESEARCH[11] SURVEY OF 147 IT DECISION-MAKERS:

- 57% of the respondents said finding and recruiting security talent was their biggest challenge
- 40% said their most inadequate security skills sets were in the areas of emerging and evolving threats
- 36% said employee turnover among security professionals was higher than in any other part of the organization
- Only one in nine expressed confidence about their ability to find security talent in future

RETHINKING YOUR BLUEPRINT

Your organization can no longer afford to treat cybersecurity as a tactical, technical function focused solely on attack prevention.

It is long past time to abandon the notion that you can defend your data and assets by just sticking them behind a firewall and using anti-malware tools to block threats from piercing your network. That model does not work on its own.

The goal of your security function must be to think as proactively as possible, with the assumption that attacks and breaches are inevitable but full-blown incidents don't have to be. You can mitigate and manage cyber risk based on a sound detection and response strategy, as well as a thorough understanding of enterprise-level impacts of security events and the likelihood of their occurrence.

To accomplish this, you can't operate in a vacuum. The security executive's role has become as much about protecting enterprise information and assets as it has about enabling business to securely take advantage of modern technologies.

10. http://www.isaca.org/About-ISACA/Press-room/PublishingImages/Cybersecurity-Infographic-large2.gif
11. https://www.trustwave.com/Company/Newsroom/News/New-Trustwave-Study-Shows-57-Percent-of-IT-Security-Professionals-Struggle-to-Find-Talent/

We know what we are, but not what we may be.

William Shakespeare

Chapter 2

Getting Business Units in Lock Step with Security

ALIGNING YOUR ORGANIZATION'S SECURITY EFFORTS WITH BUSINESS REQUIREMENTS HAS ALWAYS BEEN IMPORTANT. There is even more of a need to do so these days. Business unit decision-makers seeking to accelerate time to value are increasingly making their own technology purchase decisions, possibly leaving you in the dark. The proliferation of cloud, mobile and software as a service (SaaS) delivery models in recent years has made it easier for line-of-business units to directly acquire technologies for their needs without waiting for the IT organization's availability or approval.

DID YOU KNOW: *Non-IT business units will spend an estimated $607 billion worldwide on information technology purchases in 2017, an increase of 5.9% over last year. By 2020, line-of-business technology spending will almost equal what the IT organization spends on technology purchases.*[12]

The implications of the trend are enormous. Unsanctioned IT systems and services – commonly referred to as "shadow IT" – can open your organization to myriad security risks, including data loss and theft, data misuse and compliance problems.

The explosion of cloud services, referenced in the previous chapter, is one example. You may seriously underestimate how widespread cloud services are being used by your employees, as well as the dangers they pose. If you can't stop them, at least don't be blind to it. Throw light on the shadows by ascertaining what is being used without company approval, profiling your risk and instituting controls.

TIP: *The finance team be able to provide have a history of transactions in which technology was purchased by non-IT departments directly with the seller.*

Cloud services are not the only IT purchase that business units have begun making. Line-of-business spending on hardware, such PCs, smartphones, tablets, printers and monitors, have all been steadily increasing. Business buyers worldwide will purchase more hardware – $83.8 billion – in 2017 than IT departments will ($76.2 billion).[13]

PREDICTION: *Business buyers will spend $150.7 billion on software applications in 2017. That is more than double the $64.7 billion in software that IT organizations will buy this year.*[14]

12. IDC, "Technology Purchases from Line of Business Budgets Forecast to Grow Faster Than Purchases Funded by the IT Organization, According to IDC," March 23, 2017
13. IDC, March 23
14. IDC, March 23

A lack of IT involvement in such purchasing can result in a proliferation of non-vetted, non-standard and potentially vulnerable consumer-grade technologies in your environment.

Forward-thinking departments within your organization should not only be eager to work with the security team when making purchases, they should also feel comfortable about doing it. For example, marketing relies on platforms that contain sensitive information, and these technologies – such as content management systems – are common hacking targets. Marketers should feel empowered and encouraged to drive conversations around securing this type of infrastructure.

In general, workers want to do what is right for the company, yet often don't consider the problems that can result from their security transgressions. You can prevent this by raising their emotional commitments. Demonstrate for employees how poor security practices can lead to harm to the company and clearly articulate the level of risk their actions carry. We'll discuss some awareness training recommendations later in this e-book.

TIP: *Forming reciprocal relationships around security now will smooth the path should an incident occur later, when involvement from multiple business units will be mandatory.*

BUYING TECH: WHY YOU CAN'T SIT ON THE SIDELINES

The security team probably won't be the ones making major technology purchasing decisions. You'll be lucky to even be involved in them at all. But chances are you'll be the one left holding the bag when technologies fail and chaos erupts.

What that means is you need to be proactive about understanding what your business units want and help them achieve their objectives in a secure manner.

It means using your security smarts and experience to help business owners identify risks associated with new projects and the measures that can help mitigate those risks.

It also means getting involved in the technology purchase process, if not as the decision-maker, then at least as a trusted advisor. Your security team can help lines of business identify technologies that are secure, meet their requirements and play well with your existing infrastructure.

> *"You need to be proactive about what your business units want."*

You can inform business groups of any data protection and compliance mandates that need to be met and show them how to achieve that objective while also meeting their business goals.

There are other ways to get involved as well. Your security team can work with business units in identifying and prioritizing your most valuable data and determining the controls for protecting that information. If your organization has internal compliance and technology standards requirements, you can help different domains understand what they are and how to comply with them.

Chapter 3

Why Security Must Start with the C-Suite

INFORMATION SECURITY IS NO LONGER JUST A TECHNOLOGY ISSUE. It is an enterprise-wide imperative that requires the direct attention and the involvement of all of your corporate leaders.

Here's why:

1. The consequences of security failures have increased exponentially in recent years as companies have harnessed digital technologies to transform every aspect of their operations. Data breaches can impact business continuity, expose confidential data and intellectual property, erode customer trust, and drastically diminish shareholder value. For some, a breach can result in the worst-possible outcome: going out of business.
2. Industry mandates like the Payment Card Industry Data Security Standard and legislation like the European Union General Data Protection Regulation require organizations to adhere to standards that need to be enforced across the enterprise. Compliance failures can lead to stiff fines, business disruption, intrusive oversight measures and even prison time for executives.
3. Consumers, regulators and shareholders want CEOs and C-level executives to take more accountability for the mission of cybersecurity.

> *"What we got here is a failure to communicate."*
>
> Strother Martin — "Cool Hand Luke"

Agents of Change: Divide and Conquer

HOW THE CEO, THE CISO AND THE BOARD CAN ADEQUATELY SHARE THE SECURITY BURDEN

THE CEO CAN:

1. Assign day-to-day responsibility for the security function with someone who can be held fully accountable for executing the mission. They can ensure the individual responsible for the function gets the proper funding and support.
2. Improve security by fostering better collaboration among department leaders and stakeholders.
3. Help keep your security mission focused on business requirements. The boss can enable better security by making sure this mission is focused on increasing security maturity and risk management through improved threat protection, detection and response.
4. Engage with security executives and other stakeholders to define and communicate the organization's risk strategy and levels of acceptable risk.
5. Foster the use of meaningful metrics for measuring and managing the security program.

THE CISO CAN:

1. Develop and communicate a security mission statement rooted in business enablement.
2. Determine the risk appetite and document risk tolerance in layman's terms.
3. Choose a security framework and map initiatives to that framework.
4. Establish unbreakable rules around security responsibility and information sharing.
5. Keep owners, bosses and the board updated on security trends and be prepared to discuss specifics, such as how the organization is responding to a specific threat drawing headlines.

THE BOARD CAN:

1. Approach and understand cybersecurity as an enterprise-wide risk issue.
2. Learn the legal implications of cyber risks.
3. Access cybersecurity expertise by giving cyber risk discussions adequate time on the board meeting agenda.
4. Set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.
5. Discuss cyber risks from the perspective of identifying which risks to avoid, mitigate, accept, or transfer through insurance, as well as specific plans associated with each.

TAKING THE CUE

Many CEOs have already gotten the hint, thanks to the security trends and headlines around them. In fact, a 2016 survey of European business and IT leaders by a major insurer showed that chief executives are the ones driving the security agenda in many organizations, not the CIO or the CISO.[15]

Fifty-four percent of the 346 survey respondents said their CEO was primarily responsible for drawing up plans to protect against data breaches. In contrast, only 10 percent said their CIO was driving the security decision-making process.

Respondents cited concerns over the significant financial and business implications of breaches as the primary reason for CEOs taking charge of the security function.

CLOSING THE COMMUNICATION GAP

As a security leader, you can help your senior leaders help you by articulating your security strategy and its effectiveness in language they can understand.

Try to put yourself in their shoes. CEOs want to know how secure the organization is against cyberthreats. They want to know how effective security spending has been in reducing overall risk. They are far less interested, for example, in how many attacks you blocked at the enterprise perimeter and how many threats you detected on the production network. Unless they are security geeks at heart, that'll go right over their heads.

Unfortunately, CISOs and other security executives tend to talk technology metrics while what your boss wants to hear is business impact and risk mitigation. When CISOs present metrics to board members, the ones they think are most valuable typically are related to security incidents, data breaches and system vulnerabilities, a 2017 survey[16] by a Florida-based IT risk management firm showed. Members of the board, of whom the CEO is one, meanwhile considered metrics related to overall risk exposure, peer benchmarks and compliance as far more useful. Keep that dichotomy in mind on your next trip to the corner offices.

15. https://www.lloyds.com/news-and-insight/press-centre/press-releases/2016/09/cyber-rises-to-the-top-of-the-boardroom-agenda
16. https://go.focal-point.com/cyber-balance-sheet-report

Chapter 4

The Human Element

ONE OF THE MORE REMARKABLE ASPECTS OF SECURITY INCIDENTS IN RECENT YEARS IS JUST HOW MANY OF THEM WERE CAUSED BY HUMANS DOING THINGS THEY WOULD LATER REGRET, like clicking on malicious email attachments from strangers, leaving their laptops at an airport bar or signing into insecure wireless at the local coffee shop. As businesses have digitized more of their operations and adversaries have gotten slicker in their cons, the risks posed by such actions have increased dramatically.

Despite all the concern about zero-day vulnerabilities and sophisticated new attack methods, human error has contributed to far more breaches than anything else. In fact, an astounding nine out of 10 data breaches investigated in 2016 had a social engineering or phishing component to them.[17] In other words, these were attacks where organizations were breached, in most cases, because an employee or contractor got scammed into parting with their login credentials or downloading malware on their systems by clicking on or opening a malicious file or attachment.

> *"The human side of computer security is easily exploited and constantly overlooked."*
>
> Kevin Mitnick

THINK ABOUT IT: ***90% of all 2016 breaches happened because someone fell for a phishing email or some other social engineering gimmick.***

17. http://www.bankinfosecurity.com/interviews/most-breaches-trace-to-phishing-social-engineering-attacks-i-3516

SURVIVING BUSINESS EMAIL COMPROMISE ATTACKS

Your finance department is just as prone to lapses in judgement as anybody else. Unfortunately, the consequences of their mistakes are much greater.

The FBI estimates that U.S. businesses lost billions of dollars over the past few years in business email compromise (BEC) incidents, also known as CEO fraud or "bogus boss" scams. The hoax typically involves an authentic-looking email that appears to come from the CEO, or some other powerful executive in the organization, and is sent to an employee requesting urgent assistance to conduct a wire transfer to settle a pending invoice. Not only are the emails written convincingly thanks to meticulous reconnaissance performed by the cybercriminals behind them, but they carry the added weight of the supposed sender. When the boss has a request, employees typically act fast to satiate his or her request.

FACT: *Losses from BEC attacks, according to the FBI, increased 1,300 percent between January 2015 and February 2017. Losses from these attacks totaled more than $3 billion.*

What makes BEC scams so terrifying is that you can throw all the money in the world at technical controls to prevent them, but you can still remain as vulnerable as ever to them.

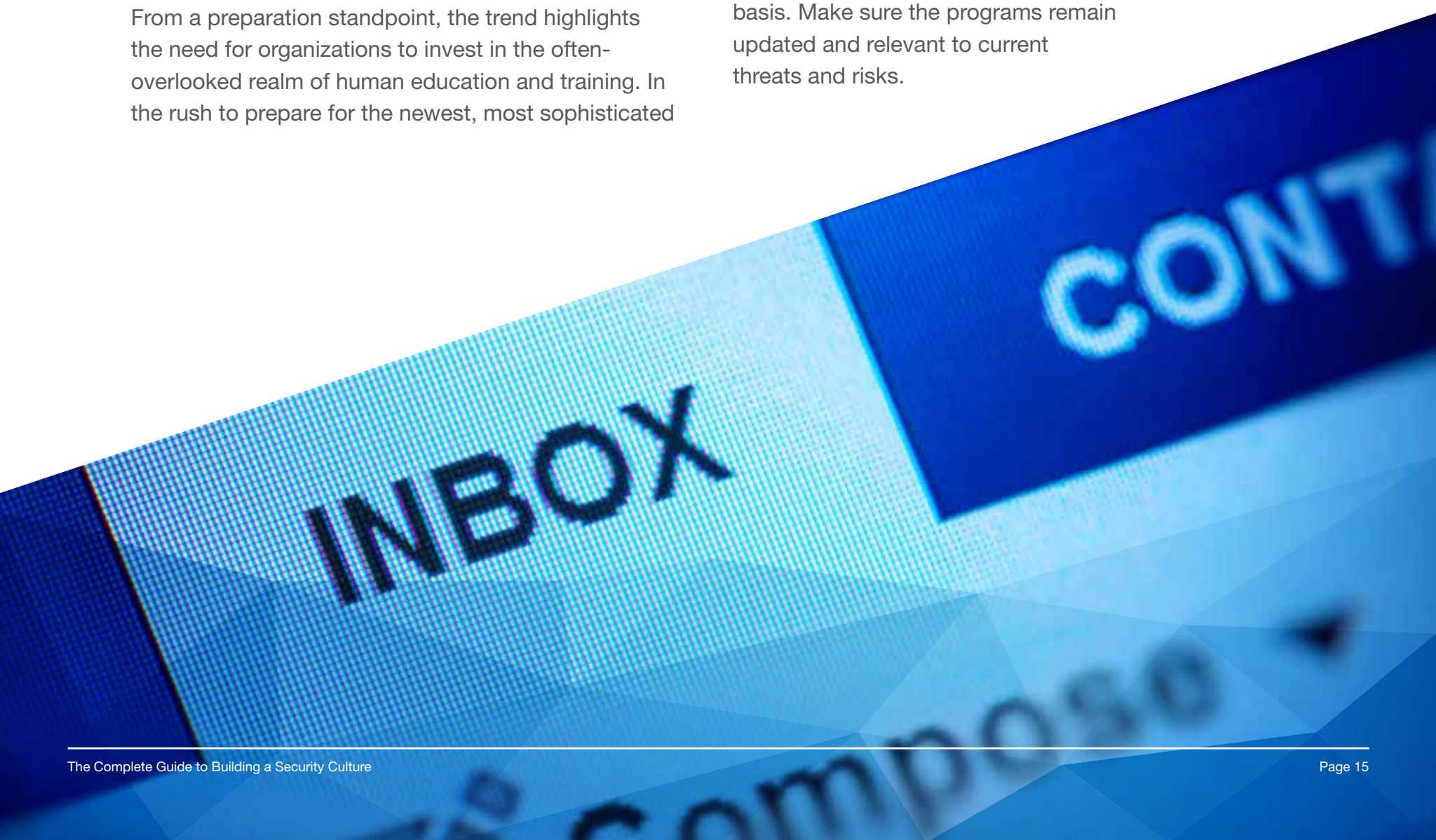
From a preparation standpoint, the trend highlights the need for organizations to invest in the often-overlooked realm of human education and training. In the rush to prepare for the newest, most sophisticated attack methods and dangerous vulnerabilities, many organizations forget that their employees are the softest target of all. Threat actors are just as apt to gain access to your network using credentials obtained from one of your employees than they are through using malware.

TIP: *If you're unsure about the payment details referenced in an email, contact the vendor to whom you allegedly owe the balance. You also should consider requiring dual-approval for all wire transfers. Finally, you can enable certain rules, like anti-spoofing and domain misspelling checks, on your email security gateway.*

Now, more so than ever, it is important to train and prepare your workers on how to recognize phishing, social engineering and other ruses designed to get them to click on malicious attachments or part with credentials.

Work with your human resources department and professional services firms as necessary to implement a formal employee cybersecurity training and security awareness program. Marketing can help give an additional leg up by providing delivery tools for helping to share your advice across the organization.

Implement a program that is consistent across your business and is conducted on a regular or an ongoing basis. Make sure the programs remain updated and relevant to current threats and risks.



How to Get Employees Excited About Security

Your employees are busy enough with their job responsibilities, they may look at security training as a big-time burden. But that's obviously not going to fly with you. For a security culture to take shape, everyone must take on some responsibility. Here are some tips for creating a security awareness program that workers won't tune out.

ESTABLISH ADVOCATES AND ACHIEVE BUY-IN

You should start by gaining support for your initiative and developing key objectives. That starts with the very top, of course, but it will really materialize when you assemble a steering committee consisting of champions from various departments.

NARROW YOUR FOCUS

There are scores of security topics you can cover in your program, but people can retain only so much knowledge. Instead, identify themes that matter most to your organization and will result in the greatest reduction of risk - keeping in mind that different departments face different risks.

CONNECT TO REAL-LIFE ATTACKS

Breaches and other security headlines are an everyday occurrence, so there are certainly enough stories you can use - even mishaps at your own organization - to add legitimacy to your awareness-building efforts.

MAKE IT ABOUT THEM

Many of the topics you will be addressing will be things employees are also familiar with when they're off the clock, such as using passwords, mobile devices and social media sites. If they feel they can apply what they learn at the office to their personal life, they'll more likely to pay attention and remember the lessons.

MAKE IT FUN, COMPETITIVE AND REWARDING

Incentives help encourage behavior changes, and some companies have turned to using gamification to make security awareness education more compelling. For example, you may award points (and prizes) to employees who flag a phishing message, while developers may compete over who can locate the most security vulnerabilities. On the flip side, employees who regularly engage in unsafe computing behavior need to hear about it too.

REINFORCE THE MESSAGE

Most experts agree than training courses won't have much effect if they are only conducted once a year. It's important not to overdo it, but reinforcement of key points is important and that can be accomplished through refresher sessions, as well as through mediums like blogs, posters and newsletters.

ENGAGE WITH YOUR BUILDERS

Aside from dispensing general awareness, you must also train developers and testers to build secure applications, products and services. Software development training helps your engineering personnel understand vulnerability prevention, assessment and remediation. And it can help meet compliance requirements.

The National Cyber Security Alliance's StaySafeOnline.org[19] campaign highlights several measures that organizations can take to bolster employee awareness of cyberthreats, including:

INSIST ON CLEAN MACHINES: Impress your employees on the importance of not downloading software from unfamiliar and unsanctioned sources. Have rules for what they can and cannot install – and enforce those rules.

IMPLEMENT STRONG PASSWORD REQUIREMENTS: Implement strong password requirements and enforce them. Better still, passphrases and two-factor authentication provide deeper protection.

EDUCATE AND REGULARLY REINFORCE: Use creative ways to teach employees about the dangers of clicking on attachments and links in emails and other messages from people they don't know.

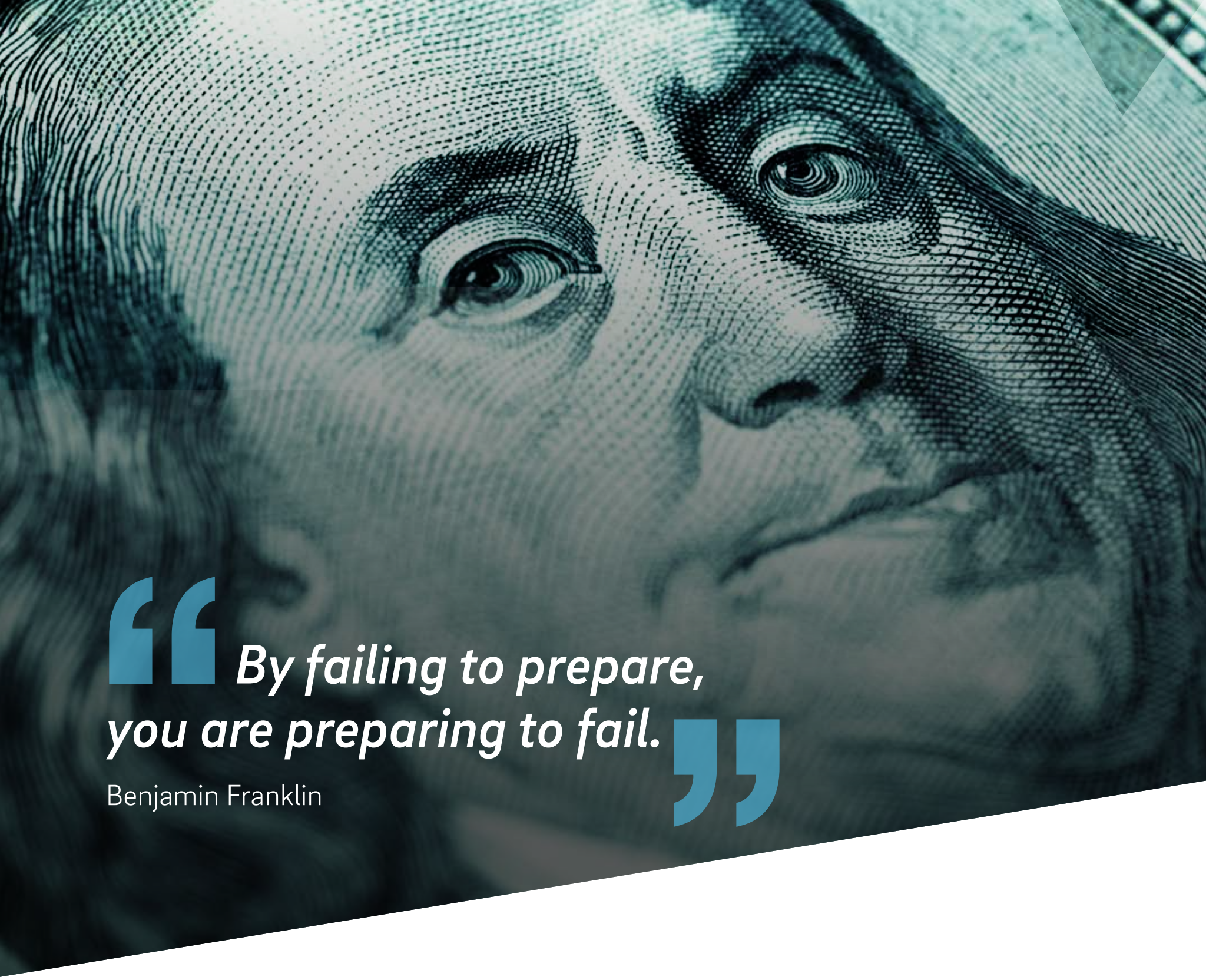
INSIST ON DATA BACKUPS: Regardless of whether you have mechanisms for doing it automatically or not, make sure your employees regularly back up their data so they have a way to recover it if bad things happen, such as ransomware incidents.

You need to decide with the HR team whether you want to make the training mandatory or optional, whether you want it to be part of the onboarding process and how you will ensure compliance with training requirements.

Consider customizing your training program for different audiences. Different business functions – and regions – within your organization handle diverse types of data. For example, HR teams deal with employee data, your marketing, customer support and sales teams handle customer data and the financial group has the account data. The way in which each group interacts with these sensitive assets are diverse and the requirements for protecting them can be unique.

FACT: *You can never generate an entirely goofproof user base. As a result, businesses are significantly increasing their spending on endpoint security,[18] including around detection and response. User endpoints are where digital marauders typically draw first blood and establish their initial foothold before advancing across your network.*

18. https://www.darkreading.com/endpoint/72--of-businesses-plan-for-endpoint-security-budget-boost/d/d-id/1329517
19. https://staysafeonline.org



Chapter 5

The Importance of Honing Incident Response

HOW YOU RESPOND TO A SECURITY INCIDENT IS AS IMPORTANT AS HOW CAPABLE YOU ARE FROM PREVENTING IT FROM HAPPENING IN THE FIRST PLACE – perhaps even more so in a world where a data breach is a virtual inevitability.

Even the most well-prepared and security-progressive organizations can experience a breach or other negative incident like a DDoS or ransomware attack. The ripple effects from such events can be felt enterprise wide and last long after the original incident itself has been mitigated.

That's why you need to know how to prepare now and react later:

1 **READINESS** You need to have a documented, well-tested incident response capability in place to deal with incidents should they happen. Readiness is as important as response. Your security team should receive training in recognizing indicators of compromise and how to respond efficiently and effectively to limit the impact of a breach, while preserving evidence and chain of custody. Simulated exercises will help you develop or tweak your response strategy and prepare staff – including personnel in other departments – to respond appropriately to a real-world scenario.

2 **RESPONSE** If an incident does occur, you will need to identify, contain and eradicate, allowing you to restore services quickly and safely. Your post-incident work will also include forensic acquisition and review – and of course – determining lessons learned. You should take away something from every incident and become more mature because of it. Like the saying goes, what doesn't break you makes you stronger.

SETTING UP A COMPUTER SECURITY INCIDENT RESPONSE PLAN (CSIRP)

As we mentioned, to develop an effective incident response capability you need to have multi-stakeholder support from across your organization. The National Institute of Standards and recommends that when you are setting up a computer security incident response plan (CSIRP), you should leverage the expertise and abilities of others in your organization, including the following:

- **YOUR SECURITY OR INFORMATION ASSURANCE TEAM,** for containing, addressing and recovering your network and services.
- **YOUR IT GROUP** for tasks such as taking systems offline quickly or implementing appropriate response measures on affected systems.
- **THE LEGAL DEPARTMENT** to handle all the potential legal ramifications of a security incident, including liability issues, evidence gathering and even the prosecution of a suspect or suspects. Your legal team can also help ensure that your incident response plan is compliant with any requirements you may be required to follow.
- **MARKETING AND PUBLIC RELATIONS STAFF** for properly communicating details of the incident, if needed, to the media and affected customers.
- **THE HUMAN RESOURCES DEPARTMENT** if an employee accidentally, negligently or maliciously caused the incident.
- **BUSINESS CONTINUITY AND DISASTER RECOVERY SPECIALISTS** to minimize operational disruption from a security incident of data breach.
- **THE CEO AND OTHER SENIOR EXECUTIVES**, as it is they who will be responsible for the incident and how your organization moves on from it.

TIP: *Considering all that is at play, more organizations than ever are turning to an external security service provider to help with planning (and, of course, response). Unless your organization is extremely well resourced, you will likely need help, especially in areas such as training, mitigation and investigation. Nail down your partner now and begin engagements with them. The last thing you want to be doing is scrambling for help in the middle of an unfolding crisis.*

TABLETOPS AND WAR GAMES

Setting up an incident response (IR) capability is a positive step – but you can't simply set it and forget it like it's a rotisserie grill being hawked on late-night infomercial. You need to routinely test your IR capability to make sure it will work if an emergency does arise. Such testing can help you identify if your detection and response capabilities work as intended and whether your incident handling, reporting and communication processes are up to snuff.

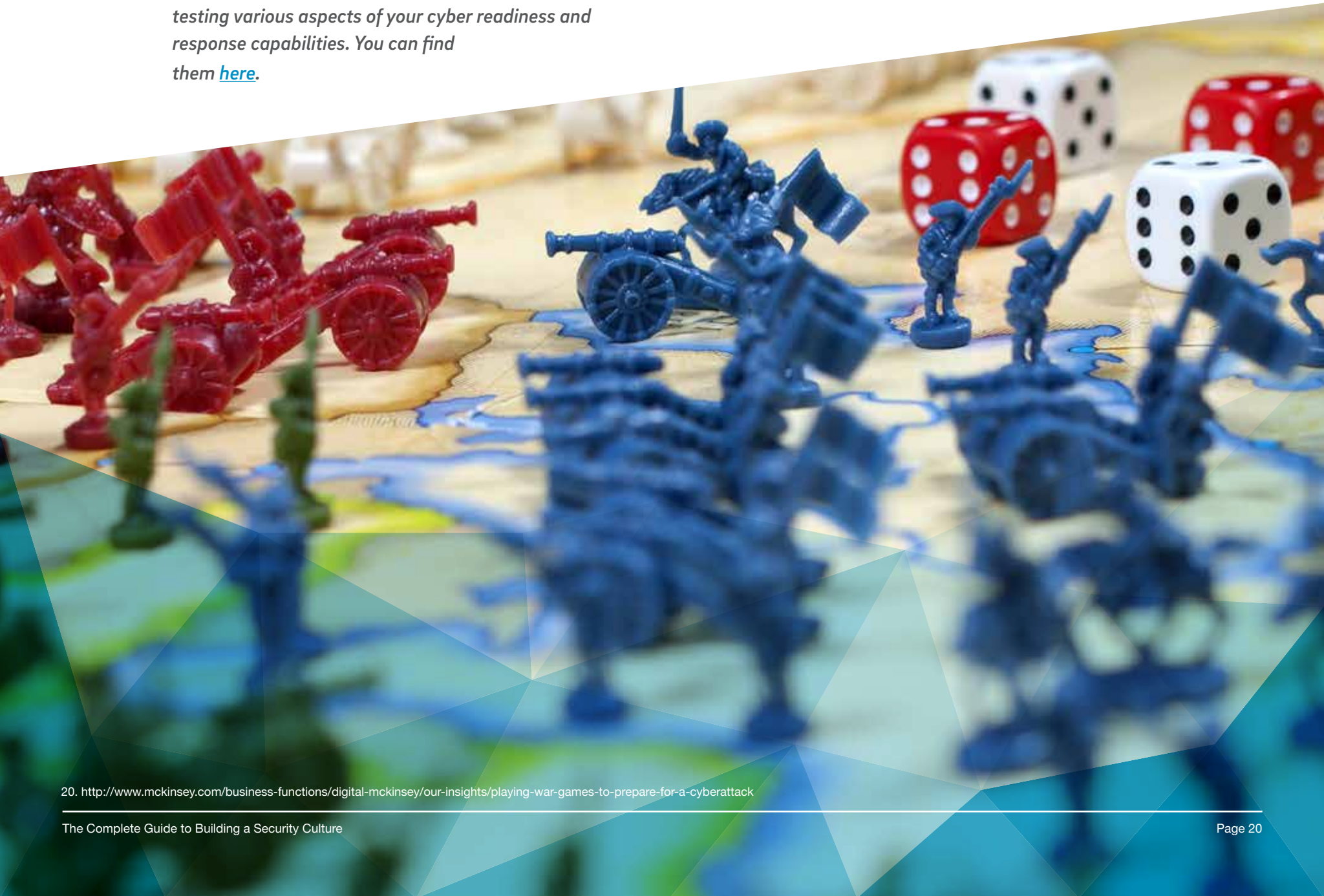
A tabletop exercise or war game that simulates a security incident at your organization is an ideal way to test how effective your plans are. Such an exercise is similar to a penetration test, but is not meant to identify technical vulnerabilities that expose your organization to risk. Rather, a tabletop exercise simulates an actual attack – such as a spear phish to top executives or a zero-day browser flaw that is being actively exploited on one of your workstations – and allows you to confront the scenario as you would the real thing…but in the comfort of a classroom setting.

TIP: *The Washington State Office of Cyber Security has a list of nearly three dozen tabletop exercises for testing various aspects of your cyber readiness and response capabilities. You can find them here.*

Typically, the exercise will involve participants from multiple business functions, including information security and IT, application development, customer support and communications. Participants will usually have some information about the simulated attack, but not all of it.

A well-structured tabletop exercise will help you identify and answer multiple questions pertaining to your incident response capabilities, including how well equipped you are to detect and respond to an incident and how effectively your team makes decisions and communicates in a crisis.[20]

Organizations with formal Red – the attacker – and Blue – the defender – teams can likely conduct these exercises on their own. In addition, there are multiple services available that offer mock exercises and help you assess your organization's readiness to respond to an incident.



20. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/playing-war-games-to-prepare-for-a-cyberattack

Chapter 6

Why Compliance Makes Cybersecurity an Enterprise Issue

> ***You are remembered for the rules you break.***
>
> Douglas MacArthur

Compliance requirements are a powerful reason to treat your cybersecurity efforts as an enterprise risk management issue, rather than as simply an IT problem. The growing use of cloud and mobile technologies has resulted in business and customer data being stored, accessed, shared and used outside the traditional enterprise firewall and more broadly than ever before.

This can create challenges and work if your organization is covered by mandates such as PCI DSS, HIPAA and SOX, which have specific requirements for protecting certain categories of data.

Violating them could mean big consequences. For example, in 2013, a major credit card association imposed a massive $13 million fine on a sportswear company that experienced an intrusion in which credit and debit card data was exposed.[25]

DID YOU KNOW? *The fines for non-compliance with payment card rules range from between $5,000 and $10,000 per month to $100,000 a month for organizations that transact a high volume of payment card data.*[26]

HIPAA GETS REAL

In 2016, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) assessed a $5.5 million penalty against a major health care provider following the theft of four laptops containing sensitive patient data. It was the largest fine ever against a single entity over a HIPAA violation, but it was by far not the only one.

A medical research institute paid $3.9 million to settle OCR's charges that it improperly disclosed personal health information (PHI) belonging to participants in a research study. One university paid $2.75 million in restitution for losing a network drive that contained PHI, while another university paid $2.7 million following the theft of a laptop containing unencrypted PHI.[21]

In all, OCR took enforcement action against a record 13 HIPAA-covered entities in 2016 and collected more than $23.4 million from them for various compliance failures. The amount represented a 300 percent increase over the previous high of $7.4 million in 2014.[22]

And the future looks bumpy. There are indications that the HHS will ramp up such enforcement actions over the next few years. The agency in 2016 offered fresh guidance on cloud computing[23] and ransomware[24] in an indication that it will be paying closer attention to these areas in future. It has also expanded the investigatory and enforcement authorities available to its regional offices.

21. http://www.hipaajournal.com/ocr-hipaa-enforcement-summary-2016-hipaa-settlements-8646/
22. https://www.law360.com/articles/885856/a-look-back-at-a-year-of-record-setting-hipaa-enforcement
23. https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
24. https://healthitsecurity.com/news/hhs-reiterates-ocr-ransomware-guidance-after-recent-attack
25. https://www.ispartnersllc.com/blog/pci-non-compliance-fines-consequences/
26. https://www.scmagazine.com/retailer-fights-pci-fines-for-noncompliance-after-breach-sues-visa/article/542261/

EMERGING REGULATIONS

Even if your organization is not covered under these mandates, there are other measures on the way.

- Financial institutions with assets of $50 billion or more could soon be subject to new security requirements from the Federal Deposit Insurance Corp. (FDIC), the Federal Reserve and the Comptroller of Currency.[27] Under the proposed plans, covered entities would be required to implement board-approved risk governance processes, have formal plans for managing risks in the workplace and supply chain, and develop processes for responding to cyber incidents.
- The U.S. Securities and Exchange Commission (SEC) wants boards and public companies to be more directly involved in their organization's cybersecurity practices.[28]
- The U.S. Federal Communications Commission (FCC) in October 2016 adopted new privacy rules that give consumers more choice and transparency over their personal data.
- The EU's General Data Protection Regulation is scheduled to take effect May 2018 and requires companies handling personal data belonging to EU citizens to implement new measures for protecting it and provide them more control over it.
- Starting in late 2017, any company that contracts with the U.S. Department of Defense will be subject to broader new security requirements.[29]

THE BOTTOM LINE

If you thought you had it bad now, your compliance obligations will likely increase over the next few years, and the consequences for failing to comply with them become more severe.

To manage these vast requirements, you must:

- Obtain a thorough understanding of the risks that face your organization.
- Identify gaps in your ability to address those risks and implement the appropriate technology measures, either internally or through partnering with a managed security services provider.
- Get a handle on your compliance requirements and ways to stay in front of any changes or additions to those requirements.
- Enable the proper compliance visibility so you know whether you are meeting requirements.
- Avoid managing compliance risk in silos. Compliance and security teams should closely work together and provide cross-department operational support.
- Develop a way to validate your compliance on an ongoing basis.

TIP *Compliance requirements can be confusing, complex and ever-changing. Remaining on top of them can be a challenge for many organizations, especially given the lack of available security skills. Unless your organization has deep pockets and a reservoir of available talent, you might find yourself needing the help of a professional services provider to manage compliance issues and responsibilities.*

27. https://washingtontechnology.com/articles/2017/02/24/insights-brown-cyber-policies.aspx
28. https://www.sec.gov/news/speech/2014-spch061014laa#.U85ghONdUfV
29. http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm

Conclusion

All Aboard the Security Train

SKILLS SHORTAGES, THE SPEED OF TECHNOLOGY CHANGE AND A CONSTANTLY EVOLVING THREAT LANDSCAPE HAVE MADE IT DIFFICULT FOR EVEN THE MOST WELL-RESOURCED ORGANIZATIONS TO SCALE SECURITY EFFORTS TO COVER ALL THEIR BASES. Adding to the burden are emerging and increasingly complex compliance requirements.

With security officially touching every part of the organization, it makes sense that it can't remain isolated in the IT department. Aside from your obvious role as attack protector, defender and responder, you also are tasked with helping to ignite and maintain a culture of security throughout the organization. The insight and advice contained in this e-book will help you kindle that flame and share the torch with others. As a final sendoff, we've condensed some of the key messages of the e-book into this nifty checklist, which you can consult at any time.

- Manage security as a function of risk (instead of merely as a technical problem) by assessing your attack surface and acknowledging your potential resource deficiencies.
- Prioritize coverage based on attacker methods, common intrusion vectors, and the most valuable systems and data you want to protect.
- Recognize that email-based malware and phishing scams are responsible for most breaches. This means your employees, from rank-and-file to the CEO, need recurrent and flexible training.
- Rally and unite departments around the importance of security by distilling technical details into information they can understand.
- Encourage departments outside of IT to be proactive about security, separate of your coordination. This will be made possible through a top-down security culture.
- Accept the reality of data breaches and concentrate increased security focus and spending around detection and response. To achieve this, you'll need to establish a cross-functional internal team that is ready to roll anytime an incident occurs.
- Build relationships with external security allies, as well. They will supplement your team with critical expertise and intelligence that will help fill your internal gaps and permit you to instead focus on revenue-generating work.

ABOUT TRUSTWAVE

Trustwave® helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit **www.trustwave.com**

Trustwave®

Smart security on demand

trustwave.com

EB-CSCYO_1117