The Executive's Breach Response Preparedness Playbook

How C-level Leaders Contribute to a Stronger Security Posture

FireEye

CONTENTS

Before a Breach

During a Breach

After a Breach

Introduction

In a recent survey, nearly 60% of enterprise respondents experienced a cyber breach.[1] Cyber breaches can significantly impact an organization. In 2017 alone, the average global cost of a cyber breach was reported at $3.62 million.[2] These costs include significant financial loss, reputational damage and possible legal ramifications which often continued long after the breach had been remediated and operations returned to normal.

Today's cyber landscape has become a matter of 'when' not 'if' a cyber breach will affect your organization. In this environment, running a successful organization requires mature cyber incident response capabilities that lead to strong organizational defense and mitigation of harmful breaches. C-suite understanding and sponsorship is critical to advance these goals.

An increasing number of regulations require C-level executives to monitor and acknowledge in writing that they understand their organization's potential security risks and have approved the established security program. Breached organizations that have violated these regulations may face sizeable penalties — tens of millions of dollars or more.

Even when organizations are well versed on the consequences of cyber breaches and not adhering to security regulations, they often struggle with identifying, prioritizing and managing cyber risks and evaluating their organization's ability to detect and respond to a cyber attack. Information technology (IT) departments can't do this alone. As cyber-attacks become more prevalent, senior executives must ensure the adequacy and effectiveness of their cyber risk management processes and IR capabilities.

This playbook is intended to help executives proactively develop and evaluate processes that strengthen their organization's cyber security posture.

Executives need to figure out what really matters to them. What are the critical assets to protect and what are the threats that are intolerable?

Kevin Mandia
Chief Executive Officer, FireEye

[1] Forrester (August 2017). Global Business Technographics Security Survey, 2017.
[2] Ponemon Institute (June 2017). 2017 Cost of a Breach Study.

CHAPTER 2

A Rapidly Growing Risk

FireEye CEO Kevin Mandia frequently states that cyber breaches are inevitable — it's not a matter of 'if,' but 'when'. There is a real need for increased focus on cyber security programs that include, or account for, IR processes as an integral component.

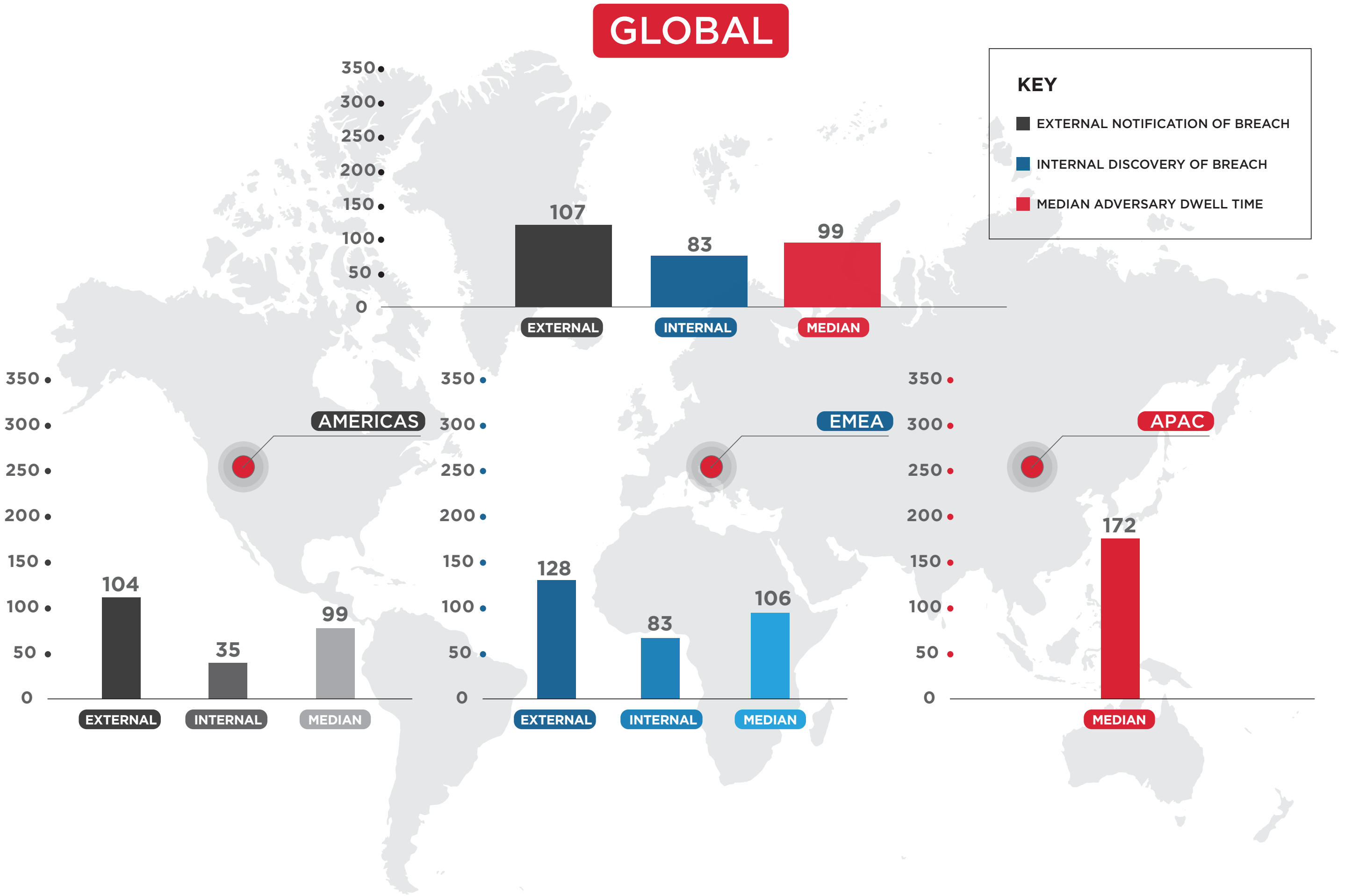
Our 2017 MTrends report showed that the median adversary dwell time is 99 days (Fig. 1) – meaning attackers have over three months within the targeted environment before a breach is even detected. Although dwell times have decreased since 2015, it is still taking organizations far too long to detect breaches. It gives attackers over 3 months of unhampered ability to quietly observe network activity, learn the inner-workings of the compromised organization, and perform reconnaissance to locate critical assets, often resulting in access and possession of sensitive data.

While all organizations are vulnerable to cyber attacks, it is important to understand that cyber risks vary by industry type.

For example, an energy company typically prioritizes keeping its oil and gas exploration and production plans secure to prevent attackers from accessing its industrial control systems. This helps them avoid operational disruptions and loss of valuable IP. Meanwhile, the main security priority at a financial institution is to safeguard against fraudulent transactions, and protect their customers' personal data so customer identities and account information cannot be accessed by threat actors.

Effective cyber security programs enable organizations to compete more assertively and position themselves as a customer advocate — vigilantly safeguarding privacy and ensuring uninterrupted operations. In today's business landscape, cyber security is a strategic imperative.

In today's business landscape, cyber security is a strategic imperative.



Financial Services:

Advanced threat actors target the financial sector in Europe for economic gain. Increased digitization of European financial institutions has made this sector a substantial target for financially-motivated cyber criminals.[3]

Energy:

Advanced Persistent Threat (APT) groups and other cyber threat actors extensively target the energy sector in the Middle East for cyber espionage and computer network attacks because of the sector's economic and strategic importance.[3]

[3] FireEye (2017). M-Trends 2017: A View from the Front Lines.

CHAPTER 3

Cyber Security Obligations by Role

Responsibility for cyber security no longer solely lies with the IT department. A strong security posture starts at the top, and must be a priority for all executives.

Each executive role has unique responsibilities for cyber risk management and a part to play in incident response.

When an organization does not have the capacity to actively occupy all C-suite roles with dedicated individuals, these responsibilities should still be considered when maturing and further developing its security posture.

CHIEF EXECUTIVE OFFICER (CEO)

A CEO coordinates with the board to emphasize organizational security, and works directly with the CISO to prioritize security as part of doing business.

CHIEF INFORMATION SECURITY OFFICER (CISO)

A CISO works closely with other C-level peers and line-of-business leaders to increase cyber risk awareness and determine cyber security needs across the organization.

CHIEF TECHNOLOGY OFFICER (CTO)

A CTO owns the vision and roadmap for the organization's technology products and services, and should consider security issues around development, review and approval processes. Ideally, the CTO and CISO collaborate closely and regularly.

CHIEF FINANCIAL OFFICER (CFO)

A CFO establishes strategic security priorities to secure financial systems and funding (as business priorities dictate), determine the business risk associated with breaches and evaluate the cost of breach remediation.

CHIEF OPERATING OFFICER (COO)

A COO works closely with the CISO to support the proper establishment, maintenance and documentation of organizational security protocols and reporting systems. At times, this role can take point on legal and regulatory compliance related to cyber security.

CHIEF MARKETING OFFICER (CMO)

A CMO serves as the communication bridge between the public, customers, partners, key stakeholders and the organization in the event of a breach. Meeting these communication demands requires pre-planning in close consultation with the CISO.

CHIEF HUMAN RESOURCES OFFICER (CHRO)

A CHRO focuses on legal, regulatory and communication issues related to the workforce, therefore making it critical to be a part of all discussions concerning breach preparedness. By working with the COO, CCO and CISO, the CHRO ensures that employee records are properly protected.

CHIEF PRIVACY OFFICER (CPO)

A CPO develops and implements policies designed to protect employee and customer data from unauthorized access. In many U.S. states and foreign countries, laws dictate security requirements for personally identified information (PII), including notification requirements when PII may be compromised.

CHIEF RISK OFFICER (CRO)

A CRO is a central figure in establishing, leading and monitoring an organization's cyber security risk management efforts. The CRO cultivates cross-departmental relationships to unify robust cyber defenses across systems (including third-party technology not governed by IT) and processes for all corporate divisions.

INFORMATION GOVERNANCE COMMITTEES

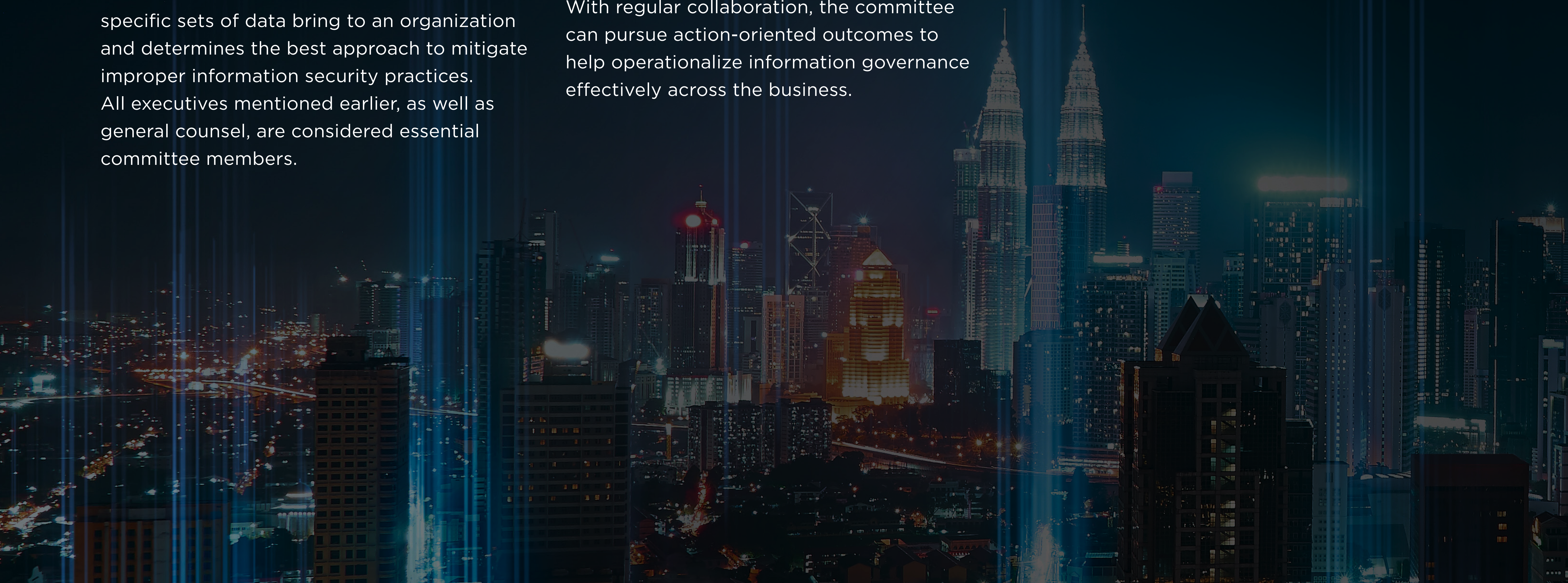
There is a need to effectively manage and govern data because as the volume of data captured and retained by companies continues to increase, so have the potential cyber risks tied to this information. This trend has become an increasingly critical concern to senior executives and board members, leading more organizations to adopt Information Governance Committees.

An Information Governance Committee evaluates the business benefits and risks that specific sets of data bring to an organization and determines the best approach to mitigate improper information security practices. All executives mentioned earlier, as well as general counsel, are considered essential committee members.

The main objectives of this committee are to:

- Manage information use and accessibility risks at the enterprise level
- Advance strategic decision making
- Apply consistent standards and recommendations across the organization

This committee should look beyond baseline documents to strategic planning, sound metrics and tools designed to achieve data management and governance objectives. With regular collaboration, the committee can pursue action-oriented outcomes to help operationalize information governance effectively across the business.



CHAPTER 4

Preparing for the Inevitable

BEFORE A BREACH

TIPS

The US Department of Homeland Security (DHS) released a list of five questions that organizations can ask themselves to assess their cyber risk:

- What are our current cyber risks and what is the potential business impact related to each risk? What is our plan to address those risks?
- How are our executives informed about cyber risks and their potential business impact to the 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 typical week? At what point is the executive team notified?
- How comprehensive is our cyber incident response plan and how often is it tested?

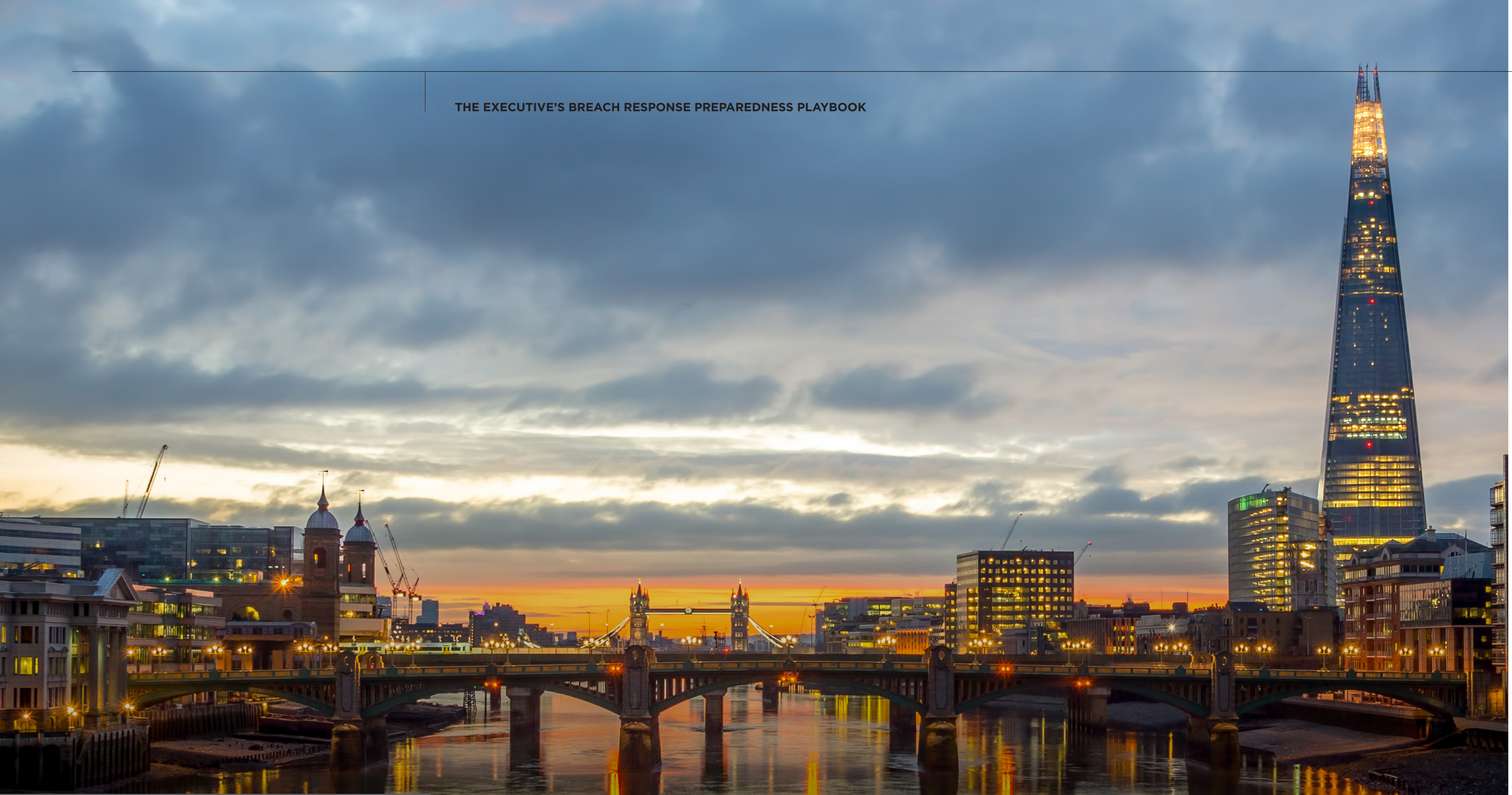
Phase 1: Assessing the Current Situation

The cyber threat landscape is changing, as attacks continuously evolve. Your organization should prepare for data breaches — and this preparation should be incorporated into your security team's daily workflow. This involves developing a coordinated response plan that considers potential cyber threats to your organization. A regular review of your organization's security strategy is a great place to start.

The use of threat intelligence regarding attacker profiles, motivations, intentions, characteristics and methods enables informed decision making when preparing for and responding to targeted attacks.

There are three types of threat intelligence: adversary, machine and victim. Adversary intelligence provides visibility into the early stages of attacker initiation — who the attackers are, what they want and what business risks they pose. Machine intelligence delivers attacker telemetry and visibility into attacker proliferation (technological methods used by attackers to copy and repeat human behavior.) Victim intelligence is based on frontline observations during an event — including attacker tools, techniques and procedures (TTPs), such as computer programming frameworks and signatures, and attacker scenarios.

The proper use of threat intelligence is essential to a strong security program. When implemented correctly, it greatly assists with risk mitigation, prioritization of events, allocation of resources and advanced IR preparedness.



Phase 1 (continued)

REGULATORY AWARENESS

Breach disclosure regulations affect most regions. The global severity of data breaches in today's cyber landscape has influenced regulators to impose bolder stakeholder notification requirements and violation penalties for organizations who undergo an incident — protecting the interest of both the business and its customers alike.

GDPR: The new General Data Protection Regulation (GDPR) affects all companies that handle EU citizens' data and will be enforced worldwide on May 25, 2018. This regulation impacts security operations, including enhanced risk detection and incident response obligations. Organizations will be required to report a data breach within 72 hours after its discovery. Violation of this could result in up to 4% of a company's global annual revenue.

TIPS

Evaluate your organization's existing threat intelligence capabilities by asking your CISO and security team these four questions:

- What are your organization's sources of cyber threat intelligence?
- How is cyber threat intelligence incorporated into our security processes?
- What threats are most relevant and why?
- What assets are these threats targeting?
- How does our organization prevent, detect and respond to these threats?

BEFORE A BREACH

Phase 2: Objectively Evaluating Your IR Capabilities

Many organizations do not clearly understand the specific business and technology risks they face. Recognizing these risk areas should influence the design of every cyber process they implement and the equipment they use.

Program Status

Start by evaluating your existing security operations center (SOC) and IR capabilities against best practices to help determine what kind of program you need and how it should evolve.

For a deeper evaluation, consider partnering with a cyber security consulting firm to assess your team's response capabilities to identify improvement opportunities.

THERE ARE MANY POPULAR AND EFFECTIVE IR ASSESSMENTS:

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 and red teaming can detail risk, likelihood of exploitation and potential business impact, and provide actionable recommendations.

Security program assessments review your security organization's practices and procedures against the latest industry standards across critical security areas (i.e., vulnerability management, risk management, access management). 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 IR capabilities for detecting and responding to attacks. They involve a comprehensive survey of your existing security event monitoring, threat intelligence and IR capabilities. The final deliverables include a security roadmap with prioritized recommendations for improvement.

TIPS

Six questions to ask your CISO and security team for an assessment of your organization's program:

- Regulatory Compliance: Do our response strategies support applicable regulatory and legal requirements?
- Staffing: Is our staff organized properly? And do they clearly understand their roles and responsibilities during an attack?
- Training: Does our staff have the training they need to respond effectively and efficiently when an incident occurs?
- Incident Detection: Does our organization have the mechanisms in place to rapidly detect an incident?
- Processes: Do we have a clear process for rapidly responding to potential data breaches?
- Technology: Do we have the necessary hardware and software to respond across the enterprise?

Phase 2 (continued)

Containment and Remediation Plans

A successful IR capability depends on establishing appropriate containment and remediation plans.

Containment plans are formalized processes to promptly contain incidents and stop threat actors from gaining access to additional networked resources. They should be specific to incident types. The goal during a containment phase is not to remove the threat from the environment, but to stop the threat from proliferating. As new threats or TTPs are discovered, containment plans should be frequently updated and maintained. Remediation plans address eradication and recovery.

These plans include developing processes for removing the threat from the environment and returning the business to normal operation while continuing to monitor for threat activity.

EXAMPLE CONTAINMENT PLANS				EXAMPLE REMEDIATION PLANS		
Blocking unauthorized outbound traffic to malicious IP addresses	Sinkholing DNS requests for malicious domains	Isolating compromised systems	Blocking all ingress and egress traffic to disconnect the company from the internet in the event of a widespread system compromise	Initiating an enterprise-wide password reset for a wide-scale employee account compromise	Developing processes that quickly disseminate patches to networked components (e.g., applications, systems, devices) impeding the threat's ability to exploit vulnerabilities and spread across the network	Developing processes that monitor remediated systems to ensure threat activity has ceased

TIPS

Questions to ask when starting to assess your organization's

Containment capabilities

- Does our security technology initiate a network block against an external IP address if unauthorized communications are identified?
- What actions does our team take to contain an incident's surge?
- Do we have the technical expertise and capability to promptly remove identified malicious emails from accounts?

Remediation capabilities

- Can we initiate an enterprise-wide account password reset task?
- Can our security team quickly apply patches to remediate an exploited vulnerability?

Phase 2 (continued)

Testing Capabilities

Practice makes perfect. Having a plan is a good starting point. Organizations can engage consulting experts to facilitate tabletop exercises that will evaluate the organization's IR plan and execution. Tabletop exercises include mock cyber attack scenarios that test the organization's IR capability. Consultants add "inserts," similar to movie plot twists, that introduce new attack developments into the scenario. Examples include website defacement, access to confidential records and the removal of sensitive data from a network.

Participants attempt to apply their current practices to discover, identify, prioritize and address the presented cyber issues. Consultants observe them to determine how their real-time decisions run concurrent to or diverge from the organization's documented plans and processes (or lack thereof), compared to industry best practices.

Recently, executives have taken a more active role in these types of exercises to gain practical cyber incident experience and enable them to recognize and prioritize necessary remediation of:

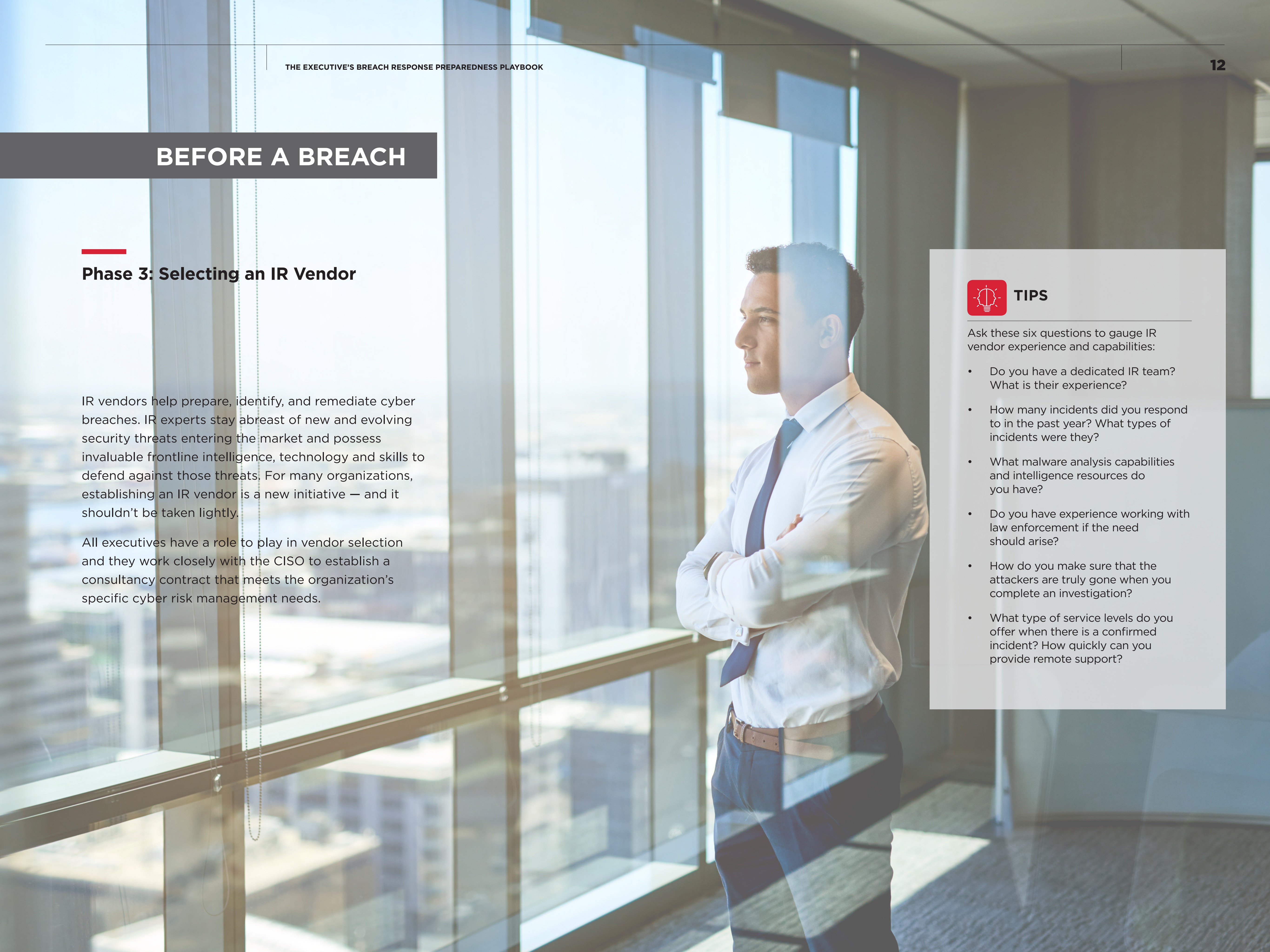
- Gaps between their security team's processes/ expectations and what actually occurs
- Deficient intelligence into real-world attacker tools, tactics and procedures
- Inability to promptly determine a cyber incident's severity

Beyond developing and practicing an IR plan, executives must continuously manage cyber risk by 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.

TIPS

To better understand the state of your IR plan and your organization's ability to support an IR investigation, your SOC and IR team can ask the following questions:

- Have playbooks been developed for rapidly deploying IR investigation tools?
- Are our data log sources collected and retained to provide responders with visibility across the environment?
- Can we provide incident responders with up-to-date documentation that details the network and endpoint architecture (for example, diagrams, security tools and controls, applications, policies and operating systems)?
- Is our security-related technology suite sufficiently documented to enable seamless deployment during an incident?
- Does a centralized asset inventory exist to identify and provide details about business-critical assets?
- Do we possess documented procedures for incident handling and escalation?



BEFORE A BREACH

Phase 3: Selecting an IR Vendor

IR vendors help prepare, identify, and remediate cyber breaches. IR experts stay abreast of new and evolving security threats entering the market and possess invaluable frontline intelligence, technology and skills to defend against those threats. For many organizations, establishing an IR vendor is a new initiative — and it shouldn’t be taken lightly.

All executives have a role to play in vendor selection and they work closely with the CISO to establish a consultancy contract that meets the organization’s specific cyber risk management needs.

TIPS

Ask these six questions to gauge IR vendor experience and capabilities:

- Do you have a dedicated IR team? What is their experience?
- How many incidents did you respond to in the past year? What types of incidents were they?
- What malware analysis capabilities and intelligence resources do you have?
- Do you have experience working with law enforcement if the need should arise?
- How do you make sure that the attackers are truly gone when you complete an investigation?
- What type of service levels do you offer when there is a confirmed incident? How quickly can you provide remote support?

Pre-Established IR Retainer Agreements

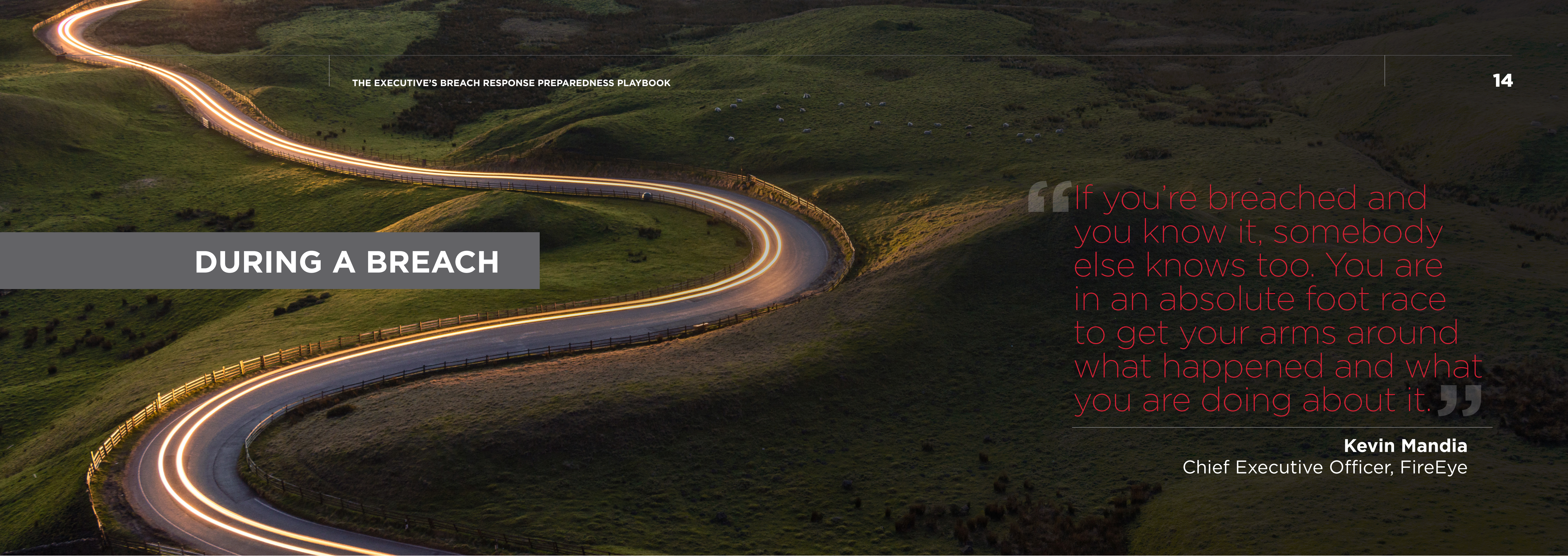
Because a breach can happen at any time, it's important to have a pre-established relationship with a credible service provider. Response speed is critical to cyber breach remediation. Adversaries may have been in your environment for weeks or months prior to detection, roaming the network and stealing sensitive data. In fact, the median dwell time of adversaries across the globe is 99 days, which gives attackers over three months of unfettered access within the target breached network. Without an established IR retainer, organizations risk undesirable and unnecessary delays before an investigation can begin.

A retainer proactively helps organizations improve their detection, response, and containment capabilities by having a trusted partner on standby. Companies should establish terms and conditions for IR services with a credible vendor before a cyber incident is suspected. This approach significantly reduces response time and minimizes the overall impact of a breach.

TIPS

Retainer agreements can be packaged in several different ways to match specific needs. When deciding which IR retainer is right for your organization, consider these important elements:

- Budget: Many vendors include prepaid hours and a pre-negotiated hourly rate if additional hours are needed during an investigation.
- Unused Hours: If prepaid hours go unused, most agreements allow you to use those hours towards proactive IR consulting services.
- Response Time: It's important to know a vendor's initial response time, as well as the timeframe guaranteed until they assign an IR responder.
- Length of Time and Payment Terms: Most retainer agreements cover a 12-month period and require up-front payment.
- Value Added Services: Some vendors include additional services with selected retainer tiers or as add-ons.
- Cyber Insurance: Most providers only reimburse you for IR expenses incurred in direct response to an incident. Some offer reduced premiums to companies that can prove they have a strong security program.



DURING A BREACH

> “If you’re breached and you know it, somebody else knows too. You are in an absolute foot race to get your arms around what happened and what you are doing about it.”
>
> **Kevin Mandia**
> Chief Executive Officer, FireEye

Crisis Communication

Determining how to disclose incident-related information outside the organization is just as important as responding to the attack.

Attempting to keep a breach quiet is no longer an option, given updated legal disclosure requirements and the likelihood that news of the event will become public from another source. In 2016, 47% of incidents investigated by Mandiant were detected by a third-party partner or law enforcement agency.[3] Whether a breach was internally or externally detected, the breached organization must be exceptionally mindful about exactly what information is disclosed, to whom and when.

Some organizations disclose as much information as possible out of their own ethical sense of corporate responsibility, while others may seek to disclose only what is required. Either way, having an established communications plan ensures that only relevant information is released to the correct authorities and the general public in a timely manner, and through the appropriate channels.

Executives should work with legal counsel and public relations partners to determine how to put the organization’s best foot forward to customers, suppliers, employees and the public — and comply with relevant laws and regulations.

In some situations, internal stakeholders may disagree about when and what to disclose. An organization’s legal counsel may declare there are specific regulatory breach disclosure rules that require the organization to notify regulatory groups within a certain amount of time after incident identification. The public relations team may want to proactively notify the public in parallel via news media, even if it is not legally required. Many executives may then ask who is notified first, the regulators or the media? The C-suite should agree on the final notification plan.

While disclosure decisions are critical, organizations must also maintain focus on the larger breach issues — gaining control of the situation, removing attackers from the organization’s network and resuming standard operations as quickly as possible.

[3] FireEye (2017). M-Trends 2017: A View from the Front Lines.

AFTER A BREACH

Looking for Improvements

Once operations return to normal after a breach, C-suite executives should ask themselves, "Could this happen again? Could this have been prevented? Could we have minimized the business impact?"

Executives need to understand how the attack happened, including what elements were weak or missing from the overall security program (and allowed the attackers to succeed) and the vulnerabilities that were exploited. This information is critical to identifying what process improvements are needed.

Areas of improvement may include enhancing firewall rulesets and upgrading security appliances that guard email, endpoints and mobile devices. For example, if an attacker gained access to the organization's network by first breaking into a partner's network, that vulnerability must be addressed. If the threat was caused by an uninformed employee who clicked on an infected link, further internal security training should be considered.

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

- A call center overwhelmed by customer queries that may indicate the need for better logistics and communications.
- Lack of knowledge about IR processes due to inconsistent response tabletop exercise facilitation or informal post-incident review activities.
- Recognition of poor security hygiene in the general workforce may spur a demand for upgraded security awareness and training.

Any breach is likely to profoundly affect your organization. Security program improvements are an essential strategic organizational priority.

Reviewing the Fine Print

Breaches can 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. Understanding the printed details falls to your legal department and COO.

CHAPTER 5

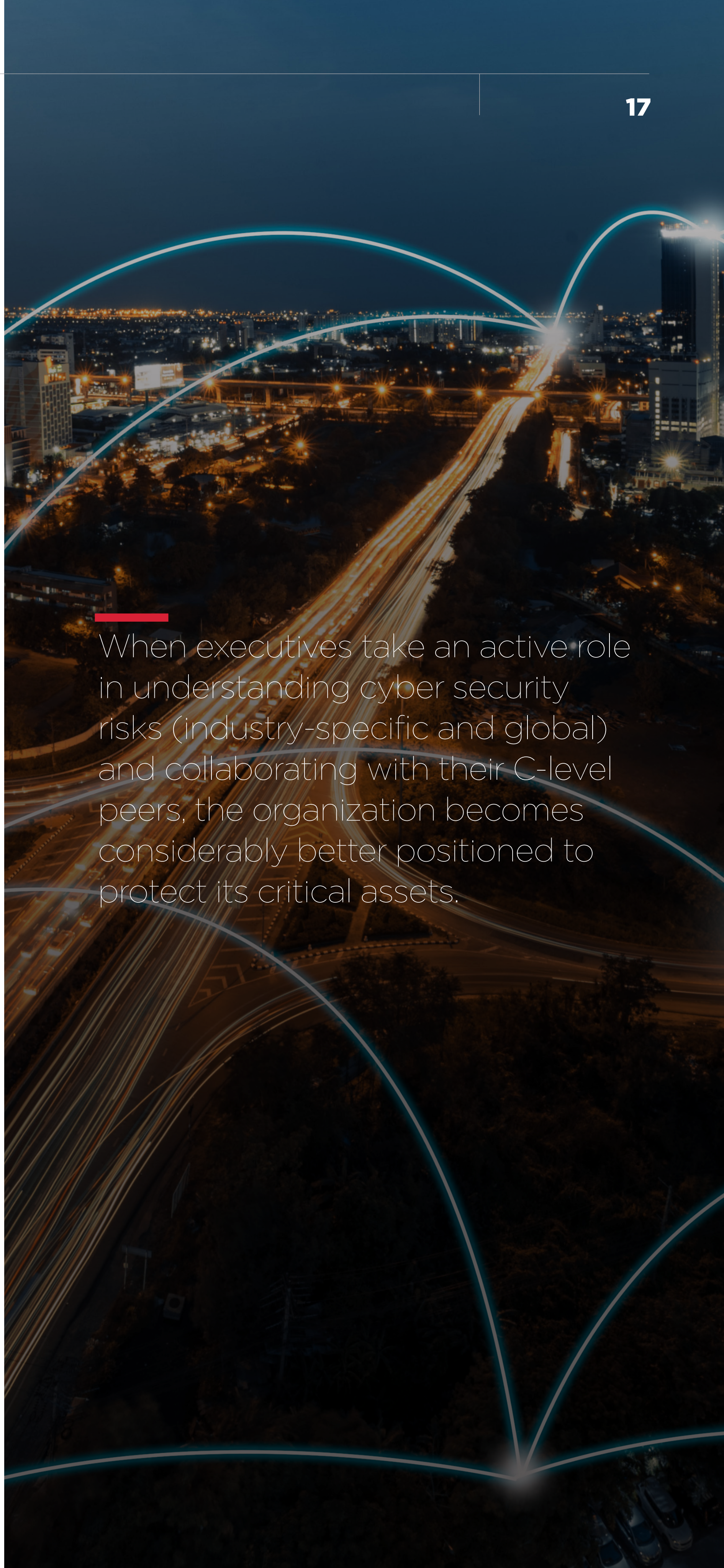
Vigilance as the New Normal

Regrettably, it takes a cyber breach for some organizations to understand the reality of constant threats in today's cyber landscape. Even when organizations survive a single incident, they must realize that the same (and new) threats will persist. Executives should never wait for a breach to establish a strong security mindset.

Your company's C-suite has an advantage if it prepares properly for a breach, responds smartly during the event, and recovers quickly after the incident. As the cyber environment becomes more precarious, every senior executive should realize their unique and critical contribution to their organization's cyber security. When executives take an active role in understanding cyber security risks (industry-specific and global) and collaborating with their C-level peers, the organization becomes considerably better positioned to protect its critical assets.

Companies are increasingly seeking advanced cyber threat intelligence concerning adversary intentions and methodologies. Most internal cyber security team's core capabilities do not encompass intelligence-gathering efforts. Therefore, establishing a relationship with an IR services provider that offers vast global intelligence resources is beneficial. This will most likely require budget shifts and strategic decision-making conversations to improve organizational protection.

By learning about and openly discussing these cyber security issues, senior leaders can help create competitive advantage through sound cyber security.



When executives take an active role in understanding cyber security risks (industry-specific and global) and collaborating with their C-level peers, the organization becomes considerably better positioned to protect its critical assets.

To learn more, visit
www.fireeye.com

FireEye is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

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

fireeye.com