Brought to you by:

mimecast

Cyber Resilience

for dummies

A Wiley Brand

Explore cyber-resilient strategies that work

Respond effectively to a cyber incident

Help your team make informed cyber decisions

Lawrence Miller
Kira Bomberg

Second Mimecast Special Edition

About Mimecast

Mimecast is a cybersecurity provider that helps thousands of organisations worldwide make email safer, restore trust and strengthen cyber resilience. Known for safeguarding customers against dangerous email, Mimecast's expanded cloud suite enables organisations to implement a comprehensive cyber resilience strategy. From AI-powered email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organisations stand strong in the face of cyberattacks, human error and technical failure.

Mimecast's customer engagement teams and Security Operations Centre help organisations of all sizes with proactive support and actionable intelligence. Our easy to use and deploy cybersecurity platform with open APIs makes customers' existing investments more valuable and cyber teams smarter. The collective intelligence gathered across our global customer base and strong partner network provides a community defence that helps make the world a more resilient place. www.mimecast.com

Cyber Resilience

Second Mimecast Special Edition

by Lawrence Miller and Kira Bomberg

for dummies®
A Wiley Brand

Cyber Resilience For Dummies®, Second Mimecast Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774, USA
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-25487-3 (pbk); ISBN 978-1-394-25488-0 (ebk)

Printed in Singapore

Publisher's Acknowledgements

Project Editor: Kerry Laundon

Acquisitions Editor: Traci Martin

Editorial Manager: Rev Mengle

Business Development Representative: Matt Cox

Content Refinement Specialist: Saikarthick Kumarasamy

Special Help: Thanks go to Garrett O'Hara for his technical review of key sections of the book.

Table of Contents

Introduction

Business leaders in all organisations must proactively plan for disruptions to their day-to-day operations. The potential impact of some of these disruptions may be limited to business operations, while others could be far-reaching, life-threatening or even cataclysmic. Cyber risks continue to rise, largely due to greater digital dependency and the interdependencies of cloud technologies.

Today, technology and cloud services have permeated every nook and cranny of our personal and professional lives. As artificial intelligence continues to evolve and become more accessible and pervasive, the risk increases for all (but mainly small) businesses who need sophisticated solutions to protect their communications, data and people.

Organisations are joined together now in massive ecosystems with their customers, vendors and partners. This has forced organisations to play more integral roles in today's digitally connected local, national and global economies. A single point of failure within an ecosystem can create a disastrous ripple effect across an entire ecosystem.

Regardless of your job role, this book provides invaluable insight into why cyber resilience is *everyone's* business, and why cyber resilience is *needed* in everyone's business.

About This Book

Cyber Resilience For Dummies, Second Mimecast Special Edition, consists of six chapters that explore:

- The importance of recovery (Chapter 1)
- Why cyber awareness is everyone's responsibility (Chapter 2)
- How to protect your business (Chapter 3)
- Why integration is key to success (Chapter 4)
- The evolution of artificial intelligence (AI) in cybersecurity (Chapter 5)
- Ten tips for a cyber-resilient business (Chapter 6)

Each chapter is written to stand on its own, so if you see a chapter that piques your interest, feel free to jump ahead. You can read this book in any order that suits you (though we don't recommend upside down or backwards).

Foolish Assumptions

This book is written primarily for readers with at least a basic understanding of IT and cybersecurity. Mainly, we assume that you are a Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Risk Officer (CRO), IT manager or system administrator. As such, an important aspect of your job is always keeping your organisation's critical systems secure and operational.

If any of these assumptions describe you, then this is the book for you! And if none of these assumptions describe you, keep reading anyway. It's a great book and after reading it, you'll be more resilient in your knowledge of cyber resilience!

Icons Used in This Book

Throughout this book, we occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out important information to commit to your non-volatile memory, your grey matter or your noggin!

TECHNICAL STUFF

If you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon *beneath* the jargon.

TIP

Tips are appreciated, never expected; we sure hope you'll appreciate these useful nuggets of information.

WARNING

Warning icons provide useful advice to keep you cyber-alert.

Beyond the Book

There's only so much we can cover in 44 short pages, so if you want to find out more, visit `mimecast.com`.

IN THIS CHAPTER

- » Understanding that cyber breaches are more likely than ever
- » Discovering the major causes of disruption
- » Combining cybersecurity with cyber resilience
- » Insuring against cyber risks

Chapter 1 When Recovery is Everything

It was once thought that cybersecurity was an area of focus for those in the IT team, or those with cybersecurity in their job title or function. In fact, until recently, 'cyber' was a language only spoken by people who worked in IT.

Today, 'cyber-speak' is used in most boardrooms, executive engagements and even among parents at soccer games. The topic has piqued everyone's interest as cyber breaches take hold of news headlines. Businesses in every country and of every size are falling victim to cyberattacks.

In this chapter, you find out the causes and adverse effects of disruption, as well as how the focus of cyber resilience (and cybersecurity strategies) has shifted from cyber breach prevention to incidence response and recovery. To protect your business, you can't just focus on cybersecurity; you need to be adaptable to pursue cyber resilience.

Embracing the Reality of Cyber Breaches

In Gartner's 2021 Maverick Research report, *You Will Be Hacked, So Embrace the Breach*, research analysts spoke of the inevitability of cyber breaches and how even the most skilled specialists and expensive technology may not be enough. Instead of working to just prevent breaches, organisations 'should focus on resilience and embrace hacks as incidents to learn from.'

In an October 2023 article, *Security* magazine reported that 'more victims were affected by ransomware in the first half of 2023 than in the entirety of 2022.'

It's fair to say that we agree with Gartner: cyber breaches are inevitable, so planning for a cyber incident to minimise disruption and abridge recovery is more important than ever. *Cyber resilience is everything.*

Gartner's report took it a step further by speaking of the mindset shift to embrace breaches, viewing them as teachable moments. Being proactive and instilling the importance of cyber resilience on your team ensures you can be prepared for the next breach and have a robust solution in place.

Causes of Disruption

According to a *Notifiable Data Breaches Report* (covering January to June 2023) from the Office of the Australian Information Commissioner (OAIC), 70 per cent of breaches were due to malicious or criminal attacks, 26 per cent occurred as a result of human error, and only 4 per cent resulted from system faults.

Bad actors

Bad actors (responsible for malicious and criminal attacks) are responsible for most cyber incidents and include cybercriminals, malicious insiders (as well as former employees/contractors), nation states, cyberterrorists and hacktivists.

For cybercriminals and malicious insiders, the motivation is usually financial gain rather than disruption, which is achieved through fraud, identity or intellectual property theft, corporate espionage or extortion (for example, ransomware). In most cases (except ransomware), their tactics are designed to evade detection for as long as possible. However, once detected, these attacks and breaches do inevitably cause some level of disruption associated with containment, eradication, remediation, recovery and investigation efforts.

For nation states, cyberterrorists and hacktivists, disruption is the name of the game. Nation states and cyberterrorists with vast financial, human and computing resources may employ advanced persistent threats (APTs) to temporarily disrupt or permanently destroy critical infrastructure. For hacktivists (and some cybercriminals), distributed denial-of-service (DDoS) attacks are used to disrupt websites and services to bring attention to a social cause, political stance or religious ideology, or to extort payment in exchange for ending the attack.

Human error

Human error accounts for around a quarter of all disruptions. Examples include incorrect configuration or use of technology or equipment by the IT team, accidental or improper sharing of sensitive information (including user accounts and confidential data), and honest mistakes due to lack of knowledge or a poor understanding of cyber threats.

REMEMBER

Human error as a cause of disruption is perhaps understandable considering human nature, but it is also alarming given that it is one of the easiest factors to address through proper training and awareness (which also helps to promote a security aware corporate culture). Read Chapter 2 for advice on practical solutions for human error.

Technology failure

Technology failure typically accounts for less than 5 per cent of disruptions. Despite this fact, disruptions due to technology failures do happen and can be very costly and destructive.

Whenever possible, single points of failure in critical systems and networks should be eliminated with resilience and redundancy. When technology failures do occur, organisations must be ready to minimise the impact of a disruption with robust data protection strategies (such as backup and recovery, and archiving) and effective disaster recovery and business continuity plans. Otherwise, employees will find temporary workarounds that may put the business at risk. For example, more than 220 million businesses worldwide rely on Microsoft Office 365 for email communications. Whenever an outage occurs, as tends to happen from time to time, staff may use personal email accounts and other non-secure communication methods to continue working, thus adding business risk on top of disruption.

Cybersecurity and Cyber Resilience: Why You Need Both

A cybersecurity strategy encompasses the technologies and processes that are designed to protect systems, networks and data from being compromised. In other words, its goal is to safeguard your data and systems from a breach or attack. Cybersecurity is a never-ending cat-and-mouse game involving new vulnerabilities and new attacks that require new technologies and new tactics, which means there will always be disruption.

REMEMBER

As a result of the ever-evolving threat landscape, things can and will go wrong. Attacks, breaches, accidents, human errors and failures will *all* happen. Disruptions are inevitable, but how you respond and how quickly you can recover is crucial. Cyber resilience focuses on ensuring business continuity by minimising the impact of disruptions, keeping critical operations running as close to normal as possible, and rapidly recovering from an incident or event.

Various cybersecurity frameworks identify different parts of the cybersecurity stack in similar terms: *prepare* (also *identify* or *discover*), *prevent* (or *protect*), *detect* and *recover* (also *respond*). In treating cybersecurity and cyber resilience as complementary strategies, you can think of *prepare* and *recover* as the cyber resilience book-ends of a cybersecurity strategy that focuses primarily on *prevent* and *detect*.

Prepare

Preparation, or some variation thereof, is typically the first part of a cybersecurity framework and is thus often logically associated with the things you do *before* an attack, breach or disruption occurs. But organisations must also prepare for what to do *during* and *after* an attack, breach or disruption.

Preparation for what happens before an attack typically involves activities such as:

- Identifying and classifying business assets (including data)
- Analysing risk based on vulnerabilities and threats
- Assessing the value and priority of business assets

Preparation for what happens during and after an attack typically includes activities such as:

- Developing incident response, business continuity and disaster-recovery plans and capabilities
- Training and testing incident response, business continuity and disaster-recovery teams
- Defining internal and external communication responsibilities and procedures

Chapter 3 talks more about cyber-protection strategies for your business.

Prevent

Prevention (or protection) is primarily focused on cybersecurity processes and technology to keep the bad stuff out. Within the realm of cyber resilience, prevention might also include designing and implementing highly resilient or redundant systems, eliminating single points of failure, and establishing alternative or contingent capabilities or processes.

Detect

Like prevention, detection is primarily a cybersecurity function. Detection typically involves developing an organisation's real-time monitoring and alerts, user and entity behaviour analytics (UEBA), and threat intelligence capabilities.

Recover

Finally, organisations need to develop a robust response capability that includes security incident response, business continuity and disaster recovery. Ultimately, it is the organisation's response capabilities that will ensure an effective cyber resilience strategy.

REMEMBER

Cybersecurity alone is no longer enough. Organisations also need to be cyber resilient, and companies with mission-critical systems, data and processes need to address both to minimise the likelihood and impact of business disruptions.

The Intersection of Risk

Hybrid working models have transformed the way organisations operate, leading to changes in how people communicate, share data and collaborate. With every new technology or tool comes a new threat surface for cybercriminals to infiltrate, creating even more risk for security leaders to manage. With the ever-increasing rise in ransomware cases, it's becoming clear that an intersection of immense risk resides between people and technology.

Today's employees are engaging across multiple communication tools at an alarming speed, often conversing on email, chat messaging platforms, social media and in virtual meetings at the same time. Devices are also being used for managing both work and personal duties in this remote, hybrid way of working, where you can log in from anywhere in the world. According to Statista, approximately 306 billion emails were sent and received every day worldwide in 2020, and this figure is projected to increase to over 376 billion daily emails in 2025. In 2018, opening emails via a desktop was already on the decline with the sharp increase of mobile phone use. Subsequently, the iPhone email app has become the most popular email client, accounting for a third of all email opens.

WARNING

To complicate this situation, your employees may often be in a hurry, on the move and stressed. Simple security measures, such as taking time to carefully preview emails before opening them — verifying the sender, hovering over links before clicking on them and considering if an attachment is safe to open — are not being prioritised in the way they once were, exposing a fundamental vulnerability for businesses of all sizes.

The Role of Cyber Insurance in Cyber Strategy

Cyber insurance is a relatively new offering in the marketplace and has been a hot topic in many boardrooms over the last decade. The first cyber insurance policies were drawn up in the late ’90s, and at first, the sector grew slowly. With the incredible rise in cyberattacks, the global market has grown considerably and is forecasted in Research and Markets’ *Global Cyber Insurance Market* 2022 report to be worth USD$20 billion by 2027. Even with today’s increased awareness of cybersecurity and a greater understanding of the risk of cyberattacks, insurance uptake has still been patchy at best.

While cyber insurance offers some peace of mind for businesses concerned with the financial impact of a breach, the premiums for cyber insurance are increasing and cyber insurance policies are becoming packed with exclusions. In fact, many insurers have begun bundling cyber insurance in with several other products or only offering limited insurance coverage, making it harder for buyers to decide what works best for them — and whether it is worth the investment.

Unfortunately, due to the cost and complexity of cyber insurance policies, many businesses don’t have cyber insurance at all. According to the Insurance Council of Australia, around 75 per cent of Australian businesses were uninsured in 2022, with the figure even higher among small and medium-sized firms.

Medibank, the victim of one of the worst cyberattacks in Australia, acknowledged that it had considered using cyber insurance before the attack, but made the decision, using its own risk assessment, to self-insure as a result of the restrictive coverage available. Medibank is not alone in making that call — and for some companies, cyber insurance is just out of reach.

As Honan Insurance Group’s Chief Executive Andrew Fluitsma commented in the *Australian Financial Review*, ‘There’ll be a number of insurance companies that won’t even look at a business that doesn’t have a bunch of security measures in place. They’ll just turn around and say, “we’re not going to insure you.”’

TIP

So, what can you do to better understand your risk profile? The best way to approach your risk profile is to

- Think like a cyber-criminal!
- Know your industry and the likelihood of being attacked.
- Understand your revenue structure and how it could be impacted by a cyberattack.
- Scope out the value of your data — that is, how much of it is considered *toxic data* (the number of sensitive records), and how you are managing that classification of your data.
- Know the cybersecurity rating or risk score associated with your supply chain. Supply chains often share network access and sensitive data, making suppliers an extension of your attack surface (your *attack surface* includes all possible points, or attack vectors, where an unauthorised user can access your system and extract data).
- Ensure that you understand the impact of a ransomware event to your business's operations.
- Conduct a FAIR risk assessment using relevant industry information, threat intelligence, risk scenarios within your business, environmental risk factors and any other data analytics to better understand your organisation's level of risk, and the financial impact of those risks. (To find out more about FAIR risk analysis, visit `fairinstitute.org`.)

Chapter 3 talks more about conducting a FAIR risk assessment and other ways to strengthen your cyber insurance strategy.

IN THIS CHAPTER

- **Taking cyber awareness training to the next level**
- **Getting your employees' attention**
- **Changing attitudes to ensure cyber compliance**

Chapter 2 Cyber Awareness is Everyone's Responsibility

In the context of cybersecurity, human error has three primary components: lack of knowledge, lack of attention and lack of concern. Individuals can suffer from a combination of these, and everyone is different.

In this chapter, discover how to address all three components to truly move the needle and change cyber behaviour.

Increasing Cyber Knowledge

These days, most businesses have some sort of cybersecurity awareness training program, and there is enough information available to employees and consumers for there to be few excuses for ignorance. Unfortunately, many of these training programs are provided infrequently and often labelled as 'boring' by employees, which consequently impacts your ability to build a cyber positive culture — and ultimately drive meaningful behaviour change.

REMEMBER

Human error is responsible for about a quarter of all breaches, according to the *Notifiable Data Breaches Report* (covering January to June 2023) from the Office of the Australian Information Commissioner (OAIC).

Your employees are also very busy. If training is too time-consuming, employees resent and avoid it. Instead, follow a micro-learning approach with training modules that take no longer than three to five minutes to complete.

Security awareness training can't be 'one and done' to be effective. Memories fade, the threat landscape changes and employees lose their shared sense of responsibility for keeping the organisation safe. Therefore, security awareness training must continually communicate and reinforce key concepts and be delivered regularly to every employee; for example, once a month. And for the employees who need a little more help — based on test results and risk scoring — they should receive targeted training as often as necessary.

TIP

Awareness training and threat intelligence help determine how vulnerable each employee is so an organisation can optimise its policies and educational programs to reduce exposure.

Some examples of relevant cybersecurity and compliance awareness training topics include:

- **Phishing.** Help people recognise possible phishing messages and show what can happen when they carelessly respond to one. The main reasons that people fall for phishing emails are curiosity, fear and urgency — so, awareness is key.
- **Ransomware.** Drive home how easy it is to get attacked, and how personally disastrous ransomware attacks can be.
- **Passwords.** Promote the use of strong passwords, such as passphrases, which are easy for employees to create — and make sure they never reuse personal passwords or write them down as a reminder. A *passphrase* is like a password but, unlike a password, it can contain spaces and is generally longer than a random string of letters, numbers or characters.

TIP

- **Data in motion.** Company data is especially vulnerable when it's in motion, and there are plenty of places it can go. You know this, but many employees don't.

- **Office hygiene.** Keep your working area clear of sensitive information and, regardless of where you're working, lock or close down your computer if you step away from it.
- **Physical security.** Beware of strangers following you into your office (tailgating) or tricking you into letting them in (it's amazing how willing people are to hold open a door for a stranger carrying a few large boxes).
- **Sharing confidential work details in public.** Talking loudly or obliviously about important, confidential work information at a café or the gym can mean other unwanted parties, such as competitors, could overhear you and act on that ill-gotten knowledge.

TECHNICAL STUFF

- **Vishing, smishing and quishing.** *Vishing* is the voice or phone call equivalent of email phishing, and *smishing* and *quishing* are its evil text message (SMS) and QR code cousins. Be sure your users understand these relatively new twists on the classic email phishing attack and how they may be caught out in their personal lives through an SMS or when wanting to access a restaurant menu via a seemingly innocent QR code.
- **Privacy.** Show how to protect everybody's personal information: your company's, your customers' and your employees'.
- **Payment Card Industry (PCI).** Help the company avoid social engineering attacks leading to financial loss and PCI non-compliance.

SMALLER BUSINESSES FACE CYBER THREATS TOO

The cybersecurity skills shortage, coupled with limited financial and technical resources, has left many companies ill-equipped to deal with the threats they face.

For example, according to the July 2022 Egnyte report *Cybersecurity Trends for Mid-Sized Organizations,* only 64 per cent of mid-sized companies have a cybersecurity incident response plan (IRP) in place. Chapter 3 talks more about IRPs.

(continued)

(continued)

Companies with fewer than 500 employees are in a similar situation, which is further compounded by the belief among business owners that they are too small to be a target. A 2022 Digital.com survey found that 51 per cent don't have any cybersecurity measures in place, while small business owners in a 2022 CNBC survey ranked inflation, supply chain disruption and labour shortages as more important concerns than cybersecurity.

Unfortunately, this deprioritisation of cybersecurity is misguided. According to the 2022 Gartner report *How to Respond to the 2022 Cyberthreat Landscape,* cybercriminals are now focusing on shorter campaigns and smaller targets, particularly when it comes to ransomware. Criminals also recognise that small businesses play an increasingly vital role in global supply chains, which makes them attractive starting points for larger-scale attacks.

The cybersecurity skills shortage also affects companies in many ways. The most common risks include misconfigured systems, incomplete risk assessments, slow patching, rushed deployments, and lack of full oversight over the security process or threat landscape.

This skills shortage also means an increased workload for talent-strapped cybersecurity teams — which often leads to burnout. Companies are then poorly positioned to respond to an ever-changing and expanding cybersecurity landscape. If smaller businesses train their entire staff to be a 'human firewall', it helps lessen the load on IT and security personnel.

REMEMBER

People can't do the right thing if they don't know what it is, and they can't avoid the wrong thing if they don't know how it makes them vulnerable. Employee security awareness training must explain what to do, what not to do and why.

Maintaining the Focus on Cyber Awareness

If all employees were always attending to security, protecting against cyber threats would be easy. But people are busy with other priorities.

To solve this problem, organisations need to get their employees' attention and keep it to help encourage the right actions when it matters.

To capture your employees' attention, try using humour and telling stories. Humans are hardwired to love stories, and a funny story is even better. Humour can consist of cartoons and caricatures, memes and recurring themes, jokes and sarcasm, and pop culture references.

Sometimes, you may also need to share some scary stories, and even have victims of cybercrimes tell your team about their experiences. The reality is that bad actors have no moral compass, and their depravity can be quite frightening when it comes to exploiting innocent victims.

Cybercriminals often launch attacks at times when people are stressed, distracted or otherwise in a hurry. This explains why there's always a flurry of cybercrime activity during peak online shopping periods, such as Black Friday and Cyber Monday. Fear of missing out (FOMO, for all you hipsters) and the pressure to buy the latest trending item often leads people to carelessly click on a 'deal of a lifetime'.

WARNING

Even worse, bad actors often use a disaster or other human crisis to exploit the humanity of others. Fake charity and fundraising websites have been set up to dupe people who think they are supporting those in need.

Unfortunately, you are likely to find many local examples without too much digging. If employees can relate to the scary stories, it may help them appreciate the importance of modifying their behaviour because they'll know how close to home these cybercriminals were able to get.

TIP

Positive reinforcement is also a great tool to help organisations motivate employees to do the right thing. Personal and public recognition of employees that demonstrate good cybersecurity practices in their day-to-day work or proactively identify potential cybersecurity issues to security staff helps to attract the attention of employees, make an emotional connection and motivate others.

Flipping the Script on Cyber Safety

Let's face it: many employees are dismissive of security. They believe you are there to get in their way and slow them down. Security always seems to be a bottleneck to productivity and the answer from the security team, no matter the question, is always 'no'. Many employees even fear interactions with the IT or cybersecurity team. Perhaps there's a stigma associated with IT and a perception that if you're getting a visit from IT security, you must've done something wrong.

To change attitudes, companies need to change the organisational culture. This begins at the top. Executives must demonstrate full support for cybersecurity initiatives by actively participating in awareness training and setting an example for the entire organisation to follow, rather than carving out C-level exceptions to cybersecurity policies and procedures. A CEO needs to be proactive when it comes to providing and participating in cybersecurity awareness training and education to staff. This sends a clear message across the entire organisation that it is incumbent upon everyone — from the top of the organisation down to junior members of staff — to equip themselves with the knowledge required to defend the network.

REMEMBER

Security teams need to change the cybersecurity paradigm. Rather than being a bottleneck to productivity, security should be a catalyst for innovation. Security, done correctly and safely, enables business agility in much the same way that brakes on a car enable you to go faster (you wouldn't go fast if you didn't have a way to stop). In this way, your employees can become human firewalls in a secure culture that protects the entire organisation.

IN THIS CHAPTER

- Minimising the threat through regular training
- Developing a robust incident response plan (IRP)
- Using phishing simulations to help employees recognise risks
- Insuring your business against cyberattacks
- Working to reduce collaboration tool risk

Chapter 3
How to Protect Your Business from Cyberattacks

Effective cybersecurity requires ongoing vigilance to ensure that you identify risks, have a response plan in place and are constantly reviewing and updating your response plan to stay ahead of evolving threats.

You can insure your business against cyberattacks, but minimising the threat and training your employees to recognise risk places you in a far better position to neutralise the threat and secure your data.

In this chapter, you discover a range of cyber-resilience strategies you can implement to protect your business.

Reducing Risky Behaviour

Different cybersecurity teams use different methods for ensuring that cybersecurity training is being adhered to but, overall, it is important that cybersecurity awareness training is measurable and that some kind of action can be taken for non-compliance. Businesses can measure the impact of their cyber-awareness training in various ways, including the use of phishing simulations and other risk-based tools (which are discussed later in this chapter). In addition, it is important that such metrics are being regularly and clearly communicated at the leadership and/or board level.

In fact, Chief Information Security Officers (CISOs) should focus their communication on the two things the board cares about most: risk and metrics.

Once a quarter, in meetings that include the heads of all business units, CISOs should report on specific results, including phishing click rates company-wide and at each business-unit level.

With regular updates, there may be less resistance to putting remediation plans into action to help get all employees operating in a more cyber-resilient way. For example, you might require that any business unit with a click rate above the company's target click rate threshold is enrolled in a 12-week cybersecurity awareness training program. You can then follow up this training with surprise testing (such as sending a fake phishing email as a test). If some employees still struggle to report or ignore phishing attempts, those employees could then participate in more intensive one-on-one coaching.

REMEMBER

Introducing a robust training program and regularly monitoring the results by testing your employees' ability to assess cyber risk can lead to significant improvements in cybersecurity and create a more cyber-secure culture.

Implementing an Incident Response Plan (IRP)

An *incident response plan* (IRP) is a guide to how an organisation will react to a cyber incident and is the first crucial step in the process of planning for and recovering from a cyberattack.

REMEMBER

Incident response planning is not a one-off exercise. Nor is it something that should be managed in isolation, because how a business responds to an incident can have a ripple effect and impact how the business is perceived by existing customers, as well as the broader market.

Gartner's 2021 Maverick Research report *You Will Be Hacked, So Embrace the Breach* gives the example of Merck, the global pharmaceutical company, which was hit by the NotPetya cyberattack — the same attack that crippled Maersk. Merck was more severely impacted because it had only applied crisis management practices to its physical assets — not its cybersecurity assets. Consequently, it wasted time arguing about whether the event was a crisis from an IT perspective. The disciplines of resilience and recovery must be applied equally across the physical and cyber domains to mitigate business risk.

REMEMBER

Bad actors don't stand still; they are constantly improving their tactics and finding new ways to attack networks. To keep up, security pros must continually evolve their defences.

Keeping your IRP current

All businesses should make it standard practice to update and test their IRPs at least once a year — and more frequently as relevant conditions change. Such conditions include:

- **Changes in the business:** Channels of communication, reporting lines and team structures may change, any of which could affect the execution of an IRP.
- **Network environment changes:** Changes to infrastructure can affect the business's security stance, so any alterations — even when they are meant to tighten security, such as adopting multi-factor or passwordless authentication — should trigger an IRP update.
- **Regulatory or compliance events:** Any scheduled reviews, audits or exercises related to the business's performance should include a review of the IRP. If, for example, a company files an initial public offering (IPO), the IRP will need to be reviewed as part of the company's preparations.

- **New threats and vulnerabilities:** The threat landscape is constantly evolving, and therefore any sign of escalations or changes in cybercriminal tactics, such as leveraging artificial intelligence (AI) or selling malware-as-a-service (MaaS), should trigger a review of the IRP.

REMEMBER

An IRP is only as good as its last test. A moment of crisis is the wrong time to realise that it falls short.

Testing and updating your IRP

Creating goals and processes is essential to the efficacy of your IRP design, and how you test and update your IRP. Clarity around the scope of testing is also necessary to uncover blind spots, security gaps and vulnerabilities.

TIP

The National Institute of Standards and Technology (NIST) has a guide to incident response testing (the *Computer Security Incident Handling Guide*) that establishes a thorough road map for setting up a test, training and exercise (TT&E) program to support the process of updating your IRP.

NIST identifies two main ways to test your IRP:

- **Tabletop exercise:** A tabletop exercise brings a group together informally, with a facilitator guiding a discussion of roles and responses in a hypothetical scenario. These exercises don't demand extensive use of resources, but they do require support from management since these exercises will involve a large group of key staff.
- **Functional exercise:** These simulations are designed to put the incident response team through its paces as if they were executing the IRP in real time. A functional exercise drills the team members in their roles, including equipment setup, forensic recordkeeping, communications and emergency notifications. The scope of these exercises can vary from a top-to-bottom response to a simulated attack through to the testing of a discrete function, such as business continuity.

The choice of testing approach may be dictated by cost (tabletop exercises are less expensive than hands-on functional exercises), objectives (functional exercises, while more time-consuming and expensive, are higher impact), and the organisation's technology maturity level.

Both forms of IRP testing involve similar steps:

- **Determine scope and goals:** Choose the broad parameters for testing, whether it's simply to check that the IRP works or to fine-tune a specific aspect, such as its activation. Then, determine the objectives, such as improving response times once a threat is detected. At this point, you may consider whether to employ an external incident response service provider. Although you cannot fully outsource this exercise, external experts could certainly help with a lot of the heavy lifting by guiding you through the process in the most efficient manner.
- **Choose the participants:** These will typically be members of the team that has to execute the IRP. Sometimes these exercises will also include members of senior management — who may have to sign off on key decisions, such as whether to pay the ransom in a ransomware attack — and senior team members responsible for certain business functions, such as legal, HR, communications and so on.
- **Design the exercise:** Depending on whether the exercise is tabletop or functional, the design may be as simple as generating a list of questions to guide a conference room discussion, or as complicated as creating virtual environments to safely simulate a data breach in real time.
- **Choose a facilitator:** The facilitator can be a member of the organisation or an outside expert who is charged with keeping a tabletop exercise moving or managing the logistics of a functional exercise. The facilitator will also maintain testing records that can be used to summarise findings and make recommendations.
- **Prepare the logistics:** Tabletop exercises require presentation materials to guide the participants, while functional exercises involve more complex preparation. This can take months, depending on the complexity of the scenario.
- **Run the exercise:** IRP testing is not a one-size-fits-all process. Every business has its own culture and priorities, and the exercise should reflect them. The approach will be shaped by your industry, company size and other factors.
- **Debrief and report:** After a tabletop exercise, the facilitator typically opens the floor to a discussion to debrief participants, collecting their impressions of what worked and what needs to be updated.

REMEMBER

All data and analysis should be collected and used to update the IRP.

- **Repeat:** Incident response testing and updating is never done. The findings of one IRP test will inform the next test.

Testing keeps your IRP sharp and up to date — and yet a 2022 Pro Research cybersecurity survey conducted by the *Wall Street Journal* revealed that although three-quarters of businesses have an IRP, less than a quarter of businesses test it regularly.

TIP

One way to free up security staff to perform regular IRP testing and updating is to leverage security automation so you can detect threats without human intervention.

Depending on the complexity of your security infrastructure, and your available resources, SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation and Response) technologies are helpful to log, orchestrate and automate cyber threats. We discuss this further in Chapter 4, where you can find out more about the benefits of an integrated security ecosystem (before diving into the role of AI in cybersecurity in Chapter 5).

REMEMBER

Email remains a main target of hackers, and technology such as email incident response tools can give security teams the bandwidth to regularly practise and hone their IRPs.

Utilising Phishing Simulations and Risk-Based Training

Generative AI is already taking phishing attacks to the next level. It lowers the barrier for cybercriminals who are not well-versed in the native language of their targets, helping them to create very convincing phishing emails. Generative AI is also providing cybercriminals with scalability, enabling them to create more customised phishing emails via *large language models*, which learn from large data sets to recognise, translate, predict or generate content.

As phishing continues to threaten most businesses, phishing simulations are being used more often as part of cybersecurity awareness training.

A *phishing simulation* is a program that businesses use to train and test employees in their ability to detect and report a variety of evolving email threats with realistic de-weaponised replications of real-world attacks.

REMEMBER

Phishing simulation programs help leaders to understand how well prepared — or not — their employees are to handle phishing attempts and provide them with an understanding of the effectiveness of their cybersecurity awareness training.

TIP

Educating employees should be the priority in any phishing simulation program. When an employee fails a phishing simulation, provide them with teachable moments in the form of bite-sized, easy-to-consume guidance to encourage behaviour change and give them the tools they need to be more cyber resilient in future.

The most effective phishing simulations are

- **Realistic:** A phishing simulation email needs to appear as true-to-life as possible, including industry-specific real-world threats that employees can expect to encounter.
- **Customisable:** Phishing simulations should include templates and campaigns that can be tailored to target the top threats to your business, unique scenarios (such as scenarios that are relevant to your industry or office location), and specific groups of individuals (such as the finance team, who may receive a fake invoice from a supplier asking that their profile be changed by adding 'new banking details').
- **Easy to use:** These simulations should be easy to configure, launch and integrate with other cybersecurity awareness training measures.
- **Measurable:** To improve future responses, phishing simulation programs need to produce data and results that can inform an organisation's training strategies and its governance, risk and compliance team.

Effectively planned and administered phishing simulations can significantly reduce workplace phishing attacks and foster a stronger security culture. However, some efforts still fall short. Common reasons for poor outcomes include programs that are

- **Too generic:** Phishing simulations need to be tailored to the groups receiving them. Marketing, for example, should receive different phishing emails than finance to expose employees to the specific threats they may encounter.

TIP

Phishing simulations should be updated to include new threats and tactics as the cybersecurity landscape evolves.

- **Too difficult:** Building security awareness doesn't happen overnight; it's a process. To build employees' confidence in spotting phishing attempts, start out with simulations that include easy-to-spot scenarios before progressing to more challenging examples.
- **Neglectful of the execs:** Executives and/or boards of directors often have high levels of access to important and valuable information, which makes them desirable targets for *whaling attacks* (a cyberattack pitched specifically at high-level executives). To improve the security awareness of senior management and board members, be sure to include these individuals in phishing simulations.
- **Too irregular:** A phishing simulation shouldn't be a one-off experience. Hold monthly trainings to keep cybersecurity top-of-mind and ensure that employees are given regular updates on new attack types.

TECHNICAL STUFF

Another risk-based or 'in the moment' training tool that has proved to be highly effective is *social graphing*, where AI uses pattern detection to flag risk in the moment. An example of this includes email banners that may alert the email recipient to the fact that the sender has never emailed the recipient before (or anyone else in the business), asking them to consider whether they are expecting that email and if they are sure that they want to click on the link in the email as it could be dangerous.

REMEMBER

As phishing attacks and resulting breaches continue to plague organisations, companies need to act to educate employees and instil best practices for recognising threats when the risk is real, not a simulation. With the right steps in place, phishing simulations can deliver lasting behavioural change and better overall cyber hygiene.

Strengthening Your Cyber Insurance Strategy

Many businesses don't have cyber insurance in place, despite the ever-increasing risk of cyberattacks — and the staggering increase in ransomware attacks is to blame. According to the *2023*

Cyber Claims Report: Mid-Year Update from cyber insurance company Coalition, ransomware claims rose 27 per cent from the second half of 2022 to the first half of 2023. The financial implications of ransomware seem to range across different markets and sizes of businesses. IBM put the average global cost of a successful ransomware attack at an eye-watering USD$4.5 million, with smaller companies being hit with five-figure demands.

When you also factor in the costs of investigation, recovery, customer support, regulatory fines, legal costs and reputational damage, it's clear that ransomware can threaten an organisation's very existence.

With this in mind, understanding the need for cyber insurance and your degree of risk can help you operate in ways that reduce the cost of cyber insurance to your business.

Evaluating the need for cyber insurance

In June 2023, Bloomberg reported that US cyber insurance premiums had surged 50 per cent in 2022 as increased ransomware attacks and online commerce drove demand for coverage. Global insurance broker Marsh said that the cost of taking out cyber cover had doubled on average every year over 2019–22.

Based on coverage, businesses may pay hundreds of thousands — if not millions — of dollars in premiums to protect them from losing ten times that (or more).

At-Bay, a cyber insurance company that positions itself as being committed to helping businesses meet digital risk, released an illuminating 2022 report, *Ranking Email Security Solutions: A Data Analysis of Cyber Insurance Claims*. The report explains that:

- Email incidents accounted for 41 per cent of their customer claims in the first half of 2022.
- Sixty per cent of email-originated claims were attributed to financial fraud.
- An email attack costs businesses an average of approximately USD$110 000, with values at the top of the range costing millions.

Careful analysis of claims data shows that the likelihood of a successful insurance claim (or multiple claims) may vary depending on the service providers the insured entity uses.

Often, cyber insurers have a pre-approved panel of service providers that are available to the insured to assist in managing an incident. These include IT forensic experts, legal advisors and PR consultants, among others. If an organisation chooses to use service providers that are not previously approved by the insurer, this could present an issue.

TIP

If you would prefer to use your own chosen service providers to respond to an incident, agree this with the insurer *before* you have an incident.

Respondents to Mimecast's *State of Email Security Report 2023* were sharply divided on the topic of cyber insurance, and whether such policies can serve as a substitute for developing a comprehensive cyber preparedness program, but most respondents strongly agreed that insurance provides a good degree of protection.

Another interesting insight from At-Bay's 2022 report suggested that 88 per cent of organisations that were inclined to reduce their reliance on cyber insurance policies also agreed that they needed to compensate by investing more in their own cybersecurity defences.

A FAIR WAY TO DETERMINE CYBER RISK

TECHNICAL STUFF

Whether you choose to have third-party cyber insurance or not, it is wise to 'think like a cyber insurer' and determine whether you (with your cyber insurer hat on) would insure your organisation or not.

To do this, you need to determine your organisation's level of risk and then translate that into financial terms (which can be quite a comprehensive task, though essential if you want a clear picture of your insurability).

The FAIR Institute (`fairinstitute.org`) is a research-driven not-for-profit organisation that has created a model for evaluating cyber risk. The Factor Analysis of Information Risk (FAIR™) model has become a game-changer in the cybersecurity environment. FAIR breaks down risk into categories and estimates their potential impact in financial terms. This helps IT and cybersecurity teams to clearly understand the threats to their business and prioritise the actions needed; it also helps businesses to develop effective risk management plans. Furthermore, as FAIR is a tool that insurers use to assess cyber risk, it is helpful to utilise this tool to develop a deeper understanding of your degree of cyber threat before you seek insurance.

Though other cybersecurity frameworks like NIST and ISO27001 are popular in the cybersecurity space, they are compliance-based approaches and have blind spots when it comes to proactively managing risk. FAIR works with these other frameworks to efficiently streamline risk compliance, risk quantification and risk assessment processes, which helps to set it apart from the rest.

Obtaining affordable cyber insurance

To give your business the best chance of securing and retaining affordable cyber insurance:

- Ensure you can explain your cyber strategy effectively, focusing on people, processes and technology.
- Check your team is equipped to deliver a quality IT or cybersecurity program that can consistently handle a number of cyber incidents on a regular basis.
- Expand your risk assessment to include your finance team, and leverage insurance brokers, your key technology partners and others that can contribute to your overall assessment of cyber risk. (The nearby sidebar ‘A FAIR way to determine cyber risk’ explains how the FAIR model can help with assessing cyber risk.)

If you can demonstrate how you address and mitigate threats across your attack surface then you will be able to:

- Provide the assurances that insurance firms require
- Manage your premium increases
- Maximise your policy limits and overall coverage
- Minimise your overall financial risk

Protecting Communications: Reducing Collaboration Risks

A new generation of collaboration tools and platforms, such as Microsoft Teams and Slack, have been quickly adopted to enable the remote- and hybrid-work models that power today's work-from-anywhere world. But these technologies have also exposed businesses to a new form of fast-rising cybersecurity risk.

In the modern work surface, few organisations can function without the use of email and collaboration tools. Software suites and their add-ons, such as Microsoft Teams, Google Workspace and Slack, integrate communications and messaging with project management functions. Designed to provide a central platform for data and document sharing, collaboration software encourages virtual teamwork and helps companies work more efficiently in the context of today's remote and hybrid working environments.

Many businesses have actively facilitated a change in the way employees communicate, seeing more traffic (and attachments) flowing through collaboration tools rather than email.

REMEMBER

Collaboration tools and platforms are catnip for cybercriminals, and many employees are ill-equipped to understand their risks. But now that organisations around the world depend on these tools, it's essential that they provide dedicated collaboration tool cybersecurity training, monitor their use of collaboration platforms, and invest in cybersecurity solutions designed to secure their collaboration and communication platforms.

Changing roles: Email versus collaboration tools

Email has shifted from being the channel for all communications to becoming the official communication platform. Communication tools like Teams and Slack have become collaborative (and conversational) hubs where message exchanges became less formal and more rapid.

These rapid message exchanges quickly evolved to include links and file sharing, resulting in privileged information flowing at scale through these collaboration tools (much as they used to primarily travel via email). The use of these tools shifted further as employees expanded *intra-organisational* collaboration to include *inter-organisational* collaboration (allowing communication both within the organisation as well as with external organisations).

Collaboration tools increase risk

As the data travelling within and between businesses has increased, the cyber risk to businesses has also increased. Data leaking out of businesses via collaboration tools is a growing concern and plagues many businesses, of all sizes, today.

Two main areas of concern are

1. **Safeguarding and archiving content:** Privileged business conversations take place through these programs.
2. **Security:** The risk of a private exchange being unknowingly infiltrated.

Gartner's 2023 *Market Guide for Email Security* stated that although email is still a significant attack vector, many attackers use email to begin the communication and then move the conversation to a collaboration platform such as Slack or Teams. The centralised infrastructure and common vulnerabilities of widely adopted collaboration and communication services offer bad actors an opportunity to focus their efforts for greater return.

In 2023, Mimecast published the global report *Collaboration Security: Risks and Realities of the Modern Work Surface*. The report shared the results of a survey that included 600 security leaders and more than 3,000 employees, and found that 94 per cent of respondents have experienced a threat via collaboration tools.

This Mimecast survey was one of the first to put a dollar value on the damages companies are incurring from collaboration tool attacks. The average cost of one of these attacks for those surveyed in 2022 was approximately USD$575 000, which includes the expense of additional security measures, added staff and systems recovery. For nearly one-third of US respondents, the financial impact climbed to more than $1 million per incident.

As with any cyber risk, human behaviour is the primary enabler of successful collaboration tool exploits. Unfortunately, it seems that employees are less likely to check the legitimacy of an unfamiliar website, attachment or source that comes their way via a collaboration platform than they are when it arrives via email. The Mimecast survey found that when using collaboration tools (compared to using email), employees were far more likely to let their guard down and perform fewer checks (such as the spelling of the source, the legitimacy of an attachment's file name and a URL's address) before clicking on any links and/or attachments.

And in the hurry to enable remote work during the pandemic, many businesses were ineffective at providing cybersecurity awareness training for the collaboration tools they were quickly rolling out.

WARNING

The lack of attention to cybersecurity training for collaboration platforms, in combination with lax employee behaviour when using these tools, is a recipe for avoidable risk.

Gartner put it best in its *Market Guide for Email Security* when it said: 'As a security and risk management leader responsible for email security, you should supplement the native capabilities of your existing cloud email solutions with third-party security solutions, to provide phishing protection for collaboration tools.'

IN THIS CHAPTER

- **Integrating your security solutions**
- **Layering your cyber defence strategies**
- **Utilising threat intelligence**

Chapter 4 The Power of Together: Integrating Security Solutions

Cyber resilience is achieved through a layered defence strategy that considers all the options you have at hand. In this chapter, you explore the benefits of a layered defence strategy, which tools you need (or may already have), and how integrating your stack of security tools can reduce complexity and ease the burden on your IT team.

Why Integration is Key

No single security solution can stop every threat. It takes a host of solutions working together to protect organisations from today's threats. Thankfully, many specialist security solutions have pre-built integrations plus example code and documentation that helps organisations easily create their own integrations, helping businesses leverage the collective power of the best-in-class technologies to reduce complexity, lower risk and optimise investments.

Integrating security products via application programming interfaces (APIs) provides a critical speed advantage in the race against adversaries so that organisations can take action before cybercriminals cause devastating damage. Manual methods of analysing and responding to threats cannot keep up with attackers' accelerating ability to find and exploit security weaknesses.

TECHNICAL STUFF

An API (*Application Programming Interface*) is a software interface that allows two applications to talk to each other. In the world of cybersecurity, APIs enable the sharing of information and suggested actions regarding cyber threats (or threat intelligence) from one security solution to another. In other words, it enables one application to ask another application to take a required action to lower MTTR (*mean time to repair or recover*) — a maintenance metric that indicates the average time taken to diagnose and rectify a fault.

Security integration has become much more critical as the complexity of organisations' technology environments have increased. Many organisations use a mixture of *best-of-suite* solutions (for example, Microsoft's range of solutions from Excel to Word, Teams, Outlook and everything in between) together with *best-of-breed* cloud-based security tools (tools that specialise in specific areas of security, such as email, endpoint security and so on, with each solution providing the best-in-class protection against a specific type of attack or threat). Too many solutions working in isolation can — counterintuitively — result in less effective security overall; therefore, connecting these often-siloed tools to share security intelligence from different areas of your ecosystem has become an essential practice.

Another approach that many organisations use is to correlate information from multiple tools using a Security Information and Event Management (SIEM) system to enrich their data and to hunt for harder-to-find threats across multiple products in a single interface. For more on SIEM, check out the nearby sidebar 'A SOARing security solution'.

REMEMBER

Leveraging APIs through integration has never been more important. By allowing security tools to exchange information in near-real time, APIs reduce the time between identifying a cyberattack and responding to the attack.

A SOARING SECURITY SOLUTION

A *Security Information and Event Management (SIEM) system* identifies and logs security events. The value a SIEM provides is storage (sometimes for compliance) and faster (perhaps even automatic) analysis of logs and telemetry at scale, with correlation across logs making it quicker for operators to identify issues and impact. This information can also be fed into a *Security Orchestration, Automation and Response (SOAR) solution* to take action. A SOAR solution is a digital framework for building workflows to automate the analysis and response of security threats at scale.

Although a SIEM system is helpful, without a SOAR, it can create manual work for the IT team and make it challenging to take the quick actions needed to protect the network. For example, if a SIEM detects a potential issue, the SOAR solution can take automated action, such as removing access for a suspicious user or isolating a malicious file.

Many organisations are now starting to move towards XDR (*extended detection and response*) or MDR (*managed detection and response*) services, which store enough of the log files (but not all) to allow for playbook-based remediation, giving you the outcome of both a SIEM (but possibly without the same level of compliance) and a SOAR (but a limited version . . . a 'SOAR-lite' solution).

Integrating Your 'Best-of-Breed' and 'Best-of-Suite' Solutions

REMEMBER

A new generation of collaboration tools and platforms have been essential to enabling today's work-from-anywhere world. But these technologies have also opened organisations up to a new form of fast-rising cybersecurity risk.

As companies adopt cloud-based collaboration technologies en masse, these platforms become high-value targets for cybercriminals seeking efficiencies of scale. Microsoft 365 has changed the digital workplace and become indispensable to most businesses, but its centralised infrastructure and vulnerabilities offer bad actors an opportunity to focus their efforts for greater return.

REMEMBER

Modern companies need to become digital fortresses, with multiple layers of proactive protection that serve to monitor, detect, alert and prevent the onslaught of cyberattacks.

Mimecast's 2023 report, *The State of Email Security*, showed:

- **94 per cent** of respondents using Microsoft 365 or Google Workspace feel that additional safeguards are needed.
- **82 per cent** of businesses reported higher volumes of email.
- **75 per cent** of businesses saw more email-based threats.
- **76 per cent** of respondents expected to face serious consequences from an email-based attack.

REMEMBER

Adopting best-of-breed security solutions is essential if you want to bolster your most vulnerable areas: endpoint, email, collaboration tools and web security. Integrating your best-of-breed tools together with a best-of-suite solution (such as Microsoft 365 or Google Workspace) makes for an even stronger defence layer where you can benefit from more visibility, threat-sharing and remediation, and get compounded value from your security stack investments.

Deriving Greater Value from Your Security Stack

In today's digital landscape, cybersecurity is increasingly important for all businesses, and while there is an obvious need for businesses to protect their networks and data, there is also the requirement for businesses to be more productive, often with reduced budgets and leaner IT teams.

Security Service Edge (SSE) is one of the many emerging concepts designed to ensure enhanced protection and improved network performance for organisations that rely on cloud-based services and virtual networking.

SSE, which includes components such as Zero Trust Network Access (ZTNA), firewall-as-a-service (FWaaS) and cloud access security broker (CASB) services, works to bring security closer to users and applications, enabling proactive threat detection, real-time monitoring, a rapid response to potential security incidents and secure access to cloud-based services.

TECHNICAL STUFF

Secure Access Service Edge (SASE) is a broader framework that encompasses the concept of SSE, integrating network and security capabilities — ideally, from as few vendors as possible. The SASE model is designed to apply network and security features as needed (and where needed) over time, making it scalable as new technology is introduced.

This scalability provides a benefit to organisations because it enables them to implement best-of-breed solutions for each of the elements of SASE, but it will also require a level of security architecture that can be fully integrated and managed.

Businesses that integrate their security solutions using SASE or SSE can then benefit from

- **Investigation and alerting:** Enhanced visibility into administrative changes, account access and the messaging lifecycle enables you to thoroughly assess the email security landscape. By integrating your security solutions using a SIEM, you're given a comprehensive view of your organisation's full security estate.
- **Threat sharing:** The combined knowledge of multiple security platforms gives you expansive protection.
- **Simplified security operations:** An integrated security ecosystem can result in the ability to block addresses, IPs and URLs, and swiftly remediate existing risks.
- **Thorough security investigations:** When looking into a potential incident, robust searching capabilities are essential.
- **Improved administration:** APIs provide the ability to perform day-to-day administration tasks with capabilities extending from adding users to managing held mail and policy modifications.

REMEMBER

The SASE framework delivers protection and performance based on the way organisations work today, with the flexibility to adapt for the changes that may arise moving forward. SASE implementation will not be easy or quick but, ultimately, organisations that can create a culture anchored in SASE will likely see benefits now and in the future.

Leveraging Threat Intelligence

Shared threat intelligence plays a critical role in keeping your business safe. Immense value comes from the bi-directional threat intelligence being shared between best-of-breed solutions. Feeding technical threat intelligence from your security platform (like your SOAR or SIEM) into a dedicated threat intelligence platform (TIP) via an integration has become a popular choice amongst organisations with mature security strategies. A TIP does the heavy lifting of providing analysis of threat data (such as its severity) to operators based on events raised in a SIEM, or being reacted to in a SOAR solution.

Manually investigating a phishing attempt could take up to 75 minutes — from creating a ticket to checking URLs, analysing the data, searching for other instances of the phishing attempt in mailboxes, communicating with others that may have been impacted and so on. Using a couple of integrated best-of-breed solutions could reduce this to two minutes from start to finish.

For example, threat intelligence may alert you to a new kind of cyberattack that's starting to wreak havoc in your industry — but hasn't yet impacted you. Learning how attackers are targeting similar organisations can help you determine whether your existing defenses are adequate or whether you need additional protection.

WARNING

Too much data can be dangerous, making it hard to see the forest for the trees. It can lead to false positives and wasted effort as organisations try to block every rumoured and actual threat that they hear about, which is something that companies can ill afford given the scarcity of security skills and the urgency of focusing on the most significant threats. Faced with a torrent of threat data, how do you decide which threats are most important to your organisation and require immediate action — and distinguish them from those that are less urgent or can be ignored altogether?

Carefully correlating and cross-checking information from multiple sources can help you decide which voices to trust, which threats to prioritise, and how much time and effort to devote to them.

IN THIS CHAPTER

- **Lifting all ships in the cyber seas using AI**
- **Detecting patterns to better protect your people**
- **Making artificial intelligence actionable intelligence**

Chapter 5 The Evolution of AI in Cybersecurity

Cyber bad actors are exploiting artificial intelligence (AI) to plot shrewder and more successful attacks. To combat this, businesses also need to incorporate AI cybersecurity solutions into their arsenals to protect themselves.

AI in cybersecurity can also be a welcome ally for overworked and understaffed cybersecurity business functions, helping them decipher the incessant wave of threats coming at them so they can focus on higher-order tasks.

Leading cybersecurity organisations are incorporating AI capabilities (such as machine learning and computer vision) into their cyber defences.

In this chapter, we discuss how the cybersecurity community has embraced artificial intelligence (AI) and explore the many applications for AI in cybersecurity, from detecting malware to predicting attacks and triaging alerts.

REMEMBER

AI is improving cybersecurity in key areas, such as threat hunting and sharing, detecting zero-day exploits and combating alert fatigue (all areas covered in this chapter). Threat intelligence sharing performs an extremely valuable preventive role in protecting your organisation against cyberattacks (Chapter 4 introduces threat intelligence, another AI-driven strategy). Analysing multiple sources of threat information can help you identify and prioritise key threats — before they impact your business.

Sifting Data for Anomalies, Social Engineering and Spam

Are AI algorithms smarter than your average security researcher? Not even close. But with certain tasks they can be cheaper, faster and more effective than many traditional analytic techniques and manual processes.

Sophisticated pattern detection is one of the best uses of AI and machine learning for cybersecurity. Cyber attackers often hide within networks and evade detection by encrypting their communications, using stolen credentials, and deleting or modifying logs. But a machine-learning algorithm designed to flag unusual behaviours can still catch them in the act.

Because machine learning excels at identifying patterns in data — much faster than a human security analyst — it can spot activity that traditional approaches miss. By continuously monitoring network traffic for variances, for example, a machine-learning model can detect risky patterns in email sending frequency that may point to the use of email for an *outbound attack* (in other words, if someone hacks one of your employees' email accounts and sends out spam or phishing attempts from that account). Models can also be programmed to watch for threats from inside your organisation (*inbound attacks*) caused by malicious employees or infiltrated accounts. What's more, machine learning can adjust to changes by ingesting new data and adapting to dynamic environments.

TECHNICAL STUFF

Deep learning, a subset of machine learning, is a statistical technique that enables computers to solve more complex problems than ever before. As the name suggests, it is more powerful than 'shallower', supervised machine learning, where the computer learns by example from labelled data. Instead, deep learning involves ingesting large quantities of data to train a deep neural network that then learns on its own, over time, how to identify images or perform other tasks. Deep learning models can achieve high accuracy rates — even for attack activities that are only vaguely defined. They can be used to better detect spam email and phishing attempts.

Another step is to surface these anomalies to employees. This may be in the form of email banner alerts that flag unexpected language, senders, attachments and so on, which brings them to the attention of the email recipient so they can take the required action (which may be disregarding the alert or reporting the threat).

REMEMBER

Training employees on how to treat such anomalies is essential to closing the security loop. Find out more about cyber-awareness training for your employees in Chapter 2.

Predicting Threats and Taking Action

Refocusing threat intelligence (refer to Chapter 4 for more on this) from identifying who is behind an attack to predicting what type of attack will occur is a better way to counter cyber threats. A predictive approach that analyses information from multiple sources enables organisations to identify and prevent cyberattacks before they happen.

REMEMBER

Predictive threat intelligence tools provide insights so that security leaders can devote more resources to protecting their company's most vulnerable targets.

A Chief Information Security Officer (CISO) can't do much to influence the efforts of would-be hackers. But what they can do is identify weak points and an attacker's most likely targets.

Threat intelligence can help you understand which employees are typically targeted and which are most at risk, so you can put the right safety nets in place. For example, instead of directly targeting well-protected senior executives, attackers may direct their phishing emails to assistants or other staff with connections to those executives. Often, business email compromise (BEC) scams impersonate executives to entice assistants to authorise money transfers or other damaging actions. You'll need to protect each link in the communication chain, not just the executive at the end of the chain.

Prevention is about user behaviour as well as technology. Analysis of user behaviour can help determine which employees present the biggest risk and where to focus your efforts. Are there employees that have previously been overlooked and need additional education or technical controls? Are some people interacting with regions that are the source of known problems? Are they repeatedly clicking on bad links?

AI in cybersecurity can also help keep the team in the security operations center (SOC) from becoming overwhelmed by non-stop incident alerts. Machine learning can step in to triage low-risk alerts, take on repetitive tasks and raise the baseline levels of threat intelligence requiring human intervention. Security professionals and analysts remain in charge, but their machine counterparts can free them up to focus on higher-level tasks and decision-making.

Hunting Zero-Day Exploits

Zero-day exploits take advantage of unknown software vulnerabilities to orchestrate a cyberattack. Defending against zero-day exploits is one of the biggest challenges for the modern cybersecurity function. In a *zero-day attack*, perpetrators introduce malware by exploiting a software vulnerability that is unknown to (or yet to be patched by) a vendor. Traditional endpoint security methods such as antivirus software or patch management solutions can't detect or prevent a zero-day exploit — it's too new for signature-based tools to catch. AI, however, may be able to help.

Deep learning architectures can be used to uncover hidden or latent patterns and become more context-aware over time — both of which are useful in identifying zero-day vulnerabilities or activities. Natural language processing can comb through source code to flag malicious files.

Coming at this from a different angle, a team at Arizona State University used machine learning to monitor traffic on the dark web to identify data relating to zero-day exploits. They've since launched a startup (CYR3CON) that uses advanced machine-learning algorithms, powered by data collected from thousands of malicious actors' posts and discussions, to predict which software weaknesses they are likely to target next. (CYR3CON has since been acquired by Cyber Security Works.)

IN THIS CHAPTER

- Translating cyber risk to business risk
- Building and maintaining strong cybersecurity practices
- Leveraging your security ecosystem for increased threat visibility
- Preparing for a breach and practising your recovery over . . . and over

Chapter 6 Ten Tips for Cyber Resilience

Here are ten tips to help your organisation increase its cyber resilience.

Communicate Identified Risks to Execs

Know your audience and wrap your message and metrics around the language your audience uses when you're sharing updates on cybersecurity threats. Boards care about 'risk' and 'metrics'; executives and business leaders focus on 'risk', 'revenue' and 'market or brand perception'. Using the right jargon can help make your communications more impactful.

Have Friends in High Places

Cybersecurity is everyone's responsibility, but it often helps to have allies across the business. Networking and influencing leaders in key business units like finance, marketing, HR and legal will help you when you need support for programs that may impact their team members.

Security Awareness is Important; Security Alertness is Critical

Cybersecurity awareness is a given these days, with increasingly high-profile cyber incidents hitting the headlines. Even so, your employees may not always be in a state of high alert (if at all) or taking the necessary steps to identify and respond to threats. Regular security awareness training (including phishing simulations and risk-based tools; refer to Chapter 3), and the results from those activities, should be baseline strategies in every business.

Two-Factor Authentication is a Must

Most financial institutions, some retailers and many other ‘end user’-focused businesses make use of two- or multi-factor authentication. Introducing a similar approach within your business is not only good security practice, but something that cyber insurers look favourably on as well.

Do the Basics Well

Focus on securing your internet-facing areas:

- Focus on identity management and authentication.
- Secure your web presence.
- Protect against advanced internet-based attacks and detect malicious intent.
- Ensure you have a layered email security solution and a multi-layered endpoint security plan.

Covering the basics effectively will be your best defence from ransomware attacks.

Create a Holistic Cybersecurity Communications Plan

A holistic, end-to-end plan maps the communications flow and encompasses:

- Employee cyber-related communications
- How internal stakeholders are updated on relevant cyber projects
- Communications to the board regarding progress on strategic initiatives
- Communications to customers and the public in the event of an incident

Patch Regularly

Patch management fixes vulnerabilities on your software and applications that are susceptible to cyberattacks, helping your business reduce its security risk.

REMEMBER

Hackers are constantly searching for vulnerabilities they can exploit, and unpatched systems and devices within your network can provide them with easy targets.

Get More from Your Security Controls with Threat Sharing

Threat intelligence plays an important preventive role by providing early warning of emerging threats before they impact your business. Specialist third-party organisations can undertake security monitoring and assessments to help gather this threat intelligence, and many of them have integrations that enable their threat feeds to flow through other tools. Correlating threat information from diverse sources can help you determine which threats to prioritise. Chapter 4 covers threat intelligence in more detail.

Identify Opportunities for Automation

It is difficult to stay on top of the growing number of security alerts that require manual analysis. The aim of security automation and orchestration is to achieve a balance between technology-driven threat responses and our ability as humans to make accurate security decisions.

TECHNICAL STUFF

As discussed in Chapter 4, a SIEM and/or SOAR solution may be worth exploring, based on the complexity of your security ecosystem and your available resources to support an array of tools.

Design, Document and Test Your Incident Response Plan

Cyber incidents are expected across all businesses, and the focus has shifted from prevention to recovery. As discussed in Chapter 3, an incident response plan (IRP) is the first crucial step in the process of planning for and recovering from a cyberattack.

REMEMBER

All businesses should make it their standard practice to update and test their IRPs at least once a year — and more frequently if relevant conditions change.

Cybersecurity is everyone's responsibility

Cyber disruption is now expected as organisations of all sizes, across the world, fall victim to increasingly sophisticated cyberattacks.

Cyber resilience helps you to minimise disruption by not only defending your business from cyberattacks but also recovering quickly from them, keeping your business running as smoothly as possible throughout. This updated book includes the latest tools and techniques that you can use to build and implement an effective cybersecurity and cyber resilience strategy.

Inside...

- Train your team to be cyber-vigilant
- Defend your organisation from phishing and ransomware
- Test and update your cyber-threat response
- Insure your business against cybercrime
- Reduce the impact of cyber disruptions
- Protect your business from cyberattacks

mimecast®

Lawrence Miller has worked in information technology for more than 25 years. He has written more than 180 *For Dummies* books on technology and security topics. **Kira Bomberg** has specialised in cybersecurity for over ten years, with a focus on coordinating global threat intelligence programs and running Customer Advisory Boards.

ISBN: 978-1-394-25487-3
Not For Resale

9 781394 254873

for dummies®
A Wiley Brand