LEARNING MADE EASY

Mimecast Special Edition

Cyber Resilience

for dummies®
A Wiley Brand

Help your team become cyber aware

Increase cyber resilience within your organisation

Protect your data and remain compliant

Compliments of

mimecast

Lawrence Miller

Daniel McDermott

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 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.

Our 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**

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cyber Resilience

Mimecast Special Edition

by Lawrence Miller and Daniel McDermott

for dummies®
A Wiley Brand

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cyber Resilience For Dummies®, Mimecast Special Edition

Published by: **Wiley Publishing Australia Pty Ltd,** 42 McDougall Street, Milton
Qld 4064

www.dummies.com

© 2020 by Wiley Publishing Australia Pty Ltd

The moral rights of the author have been asserted.

All rights reserved. No part of this book, including interior design, cover design and icons, may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Legal Services section of John Wiley & Sons Australia, Ltd, Level 2, 155 Cremorne Street, Richmond, Vic 3151, or email auspermissions@wiley.com.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Ltd., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR 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, WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANISATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANISATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

ISBN 978-0-730-38412-0 (pbk); ISBN 978-0-730-38416-8 (ebk)

Printed in Singapore

10 9 8 7 6 5 4 3 2 1

Publisher’s Acknowledgements

We’re proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organisation, contact info@dummies.biz or visit www.wiley.com/go/custompub. For details on licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Some of the people who helped bring this book to market include the following:

Project Editor: Kerry Laundon
Acquisitions Editor: Katie Mohr
Editorial Manager: Rev Mengle

Business Development Representative: Clare Dowdell
Production Editor: Mohammed Zafar Ali

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Table of Contents

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

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 and even cataclysmic. Cyber risks and stakes continue to rise, largely due to greater digital dependency, the interdependencies of cloud technologies, and increasing regulation.

Today, technology and cloud services have permeated every nook and cranny of our personal and professional lives and will become even more pervasive with new innovations such as the Internet of Things (IoT) and 5G. The sheer velocity and diversity of networked business systems has resulted in significant and ever-increasing complexity.

Organisations are now joined together in massive ecosystems with their customers, vendors and partners, forcing them to play more integral roles in digitally interconnected local, national and global economies. A single point of failure within an ecosystem could have a disastrous ripple effect across the entire ecosystem. The cyber resilience imperative has, therefore, never been greater.

About This Book

Cyber Resilience For Dummies consists of five chapters that explore:

- How to ensure operational resilience (Chapter 1)
- How to align with your business strategy (Chapter 2)
- How to address the human factor (Chapter 3)
- The need for effective governance (Chapter 4)
- Key tips for achieving cyber resilience (Chapter 5)

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

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but we assume a few things nonetheless! 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 keeping your organisation's critical systems secure and operational at all times. This book is written primarily for readers with at least a basic understanding of IT and cybersecurity.

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 quite 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 – and we sure hope you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mum warned you about (well, probably not), but they do offer practical advice.

Beyond the Book

There's only so much we can cover in 40 short pages, so if you want to learn more check out `https://getcyberresilient.com` and `https://www.mimecast.com`.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- **Recognising that disruption is the enemy**
- **Looking at the root causes of disruption**
- **Addressing resilience across the cybersecurity stack**
- **Disrupting disruption with cyber resilience**

Chapter 1 Ensuring Operational Resilience

In this chapter, you explore the causes and adverse effects of disruption. You'll also discover why you can't just focus on cybersecurity – you also need to be cyber resilient.

Disruption is the Villain

Technology is smack bang at the centre of today's very real disruption triangle, which consists of

- The continuously accelerating dependency on an organisation's own technologies and systems.
- Growing interdependencies on other organisations' cloud technologies and systems.
- Mounting industry regulation intended to protect the data residing within the technologies.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Malicious or criminal action, human error and technical failure are all security concerns that can each wreak havoc in a business. When more than one of these events occurs simultaneously there is a much greater chance for business disruption, resulting in

- Direct costs, including revenue loss and investigation, containment and recovery costs.
- Indirect costs, such as regulatory fines, legal and administrative fees, higher insurance premiums and more.
- Long-term damage to brand reputation and trust, possibly resulting in significant customer churn.

Under the worst of circumstances, significant business disruption has the very real potential of turning into cataclysmic societal disruption, where human wellbeing or lives are at stake.

CRITICAL INFRASTRUCTURE TARGETED FOR DISRUPTION

As critical infrastructure grows more digitised and interconnected, a single cyber incident has the potential to bring an entire city to a grinding halt. With the rise of the Internet of Things (IoT) and 5G in operational technology, securing critical infrastructure is a major area of active development around the world.

Australia's critical infrastructure is particularly vulnerable to cyber threats, as evidenced by the breach of the federal parliament's network and the recent cyberattack on Victorian healthcare providers.

Australia's critical infrastructure vulnerability is a symptom of a bigger problem: a Microsoft-commissioned Frost & Sullivan study, *Understanding the Cybersecurity Threat Landscape in Asia Pacific*, found that more than half of the Australian organisations surveyed have experienced a cybersecurity incident, which could cost the economy $29 billion per year.

Critical infrastructure is a target because of the massive level of disruption a single cybersecurity incident can cause. As services grow more interconnected and the IoT becomes more prevalent, power systems, transport, the internet, air traffic control and railways may become dangerously vulnerable to cyber threats.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

The challenges of securing Australia's critical infrastructure include:

- **Mixed old and new technologies.** Critical infrastructure is usually built by adding new technology on top of outmoded technology. Thus, critical infrastructure is a Frankenstein's monster of older and newer technology, which creates unique vulnerabilities.
- **Well-resourced and highly skilled attackers.** Sophisticated attackers backed by well-resourced groups (including nation states) often target critical infrastructure because of the scale of the damage it can cause.

What we can do about it

Securing critical infrastructure is an ongoing process, but starting with changes in just a few key areas can make a huge difference:

- **Operational policy.** The first step is developing a clear actionable policy for responding to critical incidents. A detailed policy should cover threat response, operational continuity, acceptable downtime and damage control, as well as standard and emergency security protocols.
- **Reputation management.** From both a compliance and communication perspective, there need to be clear guidelines on when and how to notify those affected, disclosing the details of an incident, the public relations stance to take and the community management efforts, all of which need to be clearly articulated and documented.
- **Cybersecurity and cyber resilience standards.** Given the level of interdependency in critical infrastructure, one system's vulnerability becomes everyone's vulnerability. A baseline security standard is needed, and government-mandated compliance with a standardised framework for critical infrastructure security is vital. Ensuring every critical system possesses a certain degree of resilience is essential in the event of a disruption.

Transition is always uncomfortable. Some critical infrastructure companies may feel their autonomy is being compromised and argue that the additional cost is not justified. But considering the potential damage − even loss of life − that critical infrastructure failure can cause, cyber resilience is a necessity.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Causes of Disruption

According to a recent Notifiable Data Breaches Statistics Report from the Office of the Australian Information Commissioner (OAIC), 62 per cent of breaches were due to malicious or criminal attacks, 34 per cent occurred as a result of human error, and only 4 per cent resulted from system faults.

Bad actors

Bad actors are responsible for nearly two-thirds of cyber incidents. Bad actors include cybercriminals, malicious insiders (including former employees/contractors), rogue nation states, cyberterrorists, hacktivists and <insert name of your most overrated thespian>.

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 rogue 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 approximately one-third 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 understanding of cyber threats.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

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 3 to learn how to solve 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 (see Chapter 4). Otherwise, employees will find temporary workarounds that may put the business at risk. For example, more than 220 million companies 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.

A cyber resilience strategy recognises that because of the ever-evolving threat landscape, things can, and will, go wrong. Attacks, breaches, accidents, human errors and failures will all happen, and disruptions are inevitable. Cyber resilience focuses on ensuring business continuity by minimising the impact of disruptions,

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

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 *respond* (also *recover*). In treating cybersecurity and cyber resilience as complementary strategies, you can think of *prepare* and *respond* 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

Prevent

Prevention (or protection) is primarily focused on cybersecurity processes and technology – that is, keeping 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.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

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.

Respond

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 Cyber Resilience Imperative

Nearly all cyberattacks today leverage email. According to research by PhishMe, 91 per cent of cyberattacks start with phishing emails. Why? Email is always on, it’s a trusted communication channel within and between organisations, it can be used to send malicious links and attachments, and it can be easily impersonated. Therefore, email is a cheap, simple and highly effective tool for bad actors who want to:

- Gain control over an organisation’s IT assets
- Access and steal sensitive information (including using an organisation’s brand to defraud its customers)
- Disrupt business operations

With email being the primary form of communication for most businesses and the single largest attack vector today, cyber resilience needs to begin with strong email security.

Email security has traditionally been provided by a secure email gateway, a classic email perimeter strategy to keep bad emails from making their way to corporate mailboxes. However, changes in the modern threat landscape require that the strategy extends beyond this perimeter-based approach to an email security strategy that is more pervasive, multi-zoned and integrated with a company’s

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

overall security systems. Importantly, such a strategy must extend the security for, and add protection to, cloud-based services such as Microsoft Office 365 and Google Mail (Gmail).

At the perimeter

Attackers send spam and viruses via email and embed links in email to conduct phishing and spear phishing attacks. They also deliver forms of malware that organisations can't detect with traditional signature-based antivirus technologies.

Email messages come in and very often go out of organisations at the network perimeter through an email gateway. The email perimeter is a very important place to concentrate security controls, including looking for malware or phishing threats and applying content controls.

Inside the perimeter

Even with a robust email security perimeter in place, attackers are often able to breach the perimeter and infiltrate a network. They can then use compromised employee accounts or social engineering to transmit malicious emails from an internal network. Your cyber defences are only as strong as your weakest link – which is often human error on the part of an unaware, inattentive or apathetic employee. Read Chapter 3 to find out why you need to create a *human firewall* through cyber aware and smart staff.

Organisations should employ many of the same robust email security technologies they use at the perimeter to inspect internal traffic. Importantly, inappropriate or malicious content should be immediately extracted from the network once detected. By applying automated threat detection with multiple scanning technologies to internally generated email traffic, organisations can detect, analyse and remediate threats in their email systems.

Beyond the perimeter

It's incredibly easy for an attacker to impersonate an organisation on the internet without even bothering to breach the organisation's perimeter or infiltrate its network. Attackers can leverage a brand's reputation and ultimately destroy the value and trust that an organisation may have taken years or decades to build. Even an unsophisticated attacker can simply register a similar domain name or host a website or login page to lure unsuspecting customers, partners or the general public. The cost to a business and its customers can be devastating.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- **Assessing business impact**
- **Ensuring regulatory compliance at all times**
- **Calculating the cost of downtime**

Chapter 2 Aligning Cybersecurity with Your Organisational Strategy

n this chapter, you explore the potential impact of a disruption to your business, as well as compliance considerations and the cost of downtime.

Understanding the Potential Business Impact of Disruption

Email is always on. It's a trusted communication channel within and between organisations, it can carry links and attachments, and it can be easily impersonated. All of this makes email a cheap, simple and highly effective tool for bad actors who want to do one or all of the following:

- Access and steal sensitive information
- Impersonate an organisation's brand to defraud its customers

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Take control of an organisation's IT assets
- Disrupt business operations

There are far too many examples of organisations that have been breached using email as the attack vector, all with devastating business impacts. Some recent cases include:

- **Victoria hospitals.** Various hospitals and health facilities across regional Victoria were targeted by cyber attackers in October 2019. Although it appears that no patient information was compromised, ransomware blocked access to several systems, including patient record, booking and management systems, which negatively impacted patient contact and scheduling in some locations. Among those affected was Barwon Health – University Hospital in Geelong, requiring the health service's entire network to be shut down to contain the effects of the attack.
- **Toll Group.** In January 2020, Australian transport and logistics company Toll Group was hit by a ransomware attack that is believed to have infected as many as 1,000 servers, forcing them to shut down most of their IT infrastructure to prevent the malware from spreading further. For several weeks, the company was forced to rely on a combination of automated and manual paper-based processes, causing delivery delays and preventing customer access to services such as freight, parcels, warehousing and logistics, and forwarding operations across Toll Group's global network. In addition to the costs of delivery delays, interruption of service and downtime, the company is also dealing with potential long-term brand reputation damage due to the attack.
- **DLA Piper.** Global law firm DLA Piper was hit by the destructive NotPetya malware in June 2017. Despite identifying the attack within the first 20 minutes of infection, all of the firm's data centres and Windows-based servers worldwide were impacted within 48 hours. During the first three weeks of the recovery effort, the IT team put in over 15,000 hours of overtime, and it soon became evident that nothing in the existing environment could be salvaged. The firm ultimately had to rebuild its entire Windows environment anew.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Australian National University (ANU).** In November 2018, a malicious email sent to a senior staff member compromised the ANU network – without even needing anyone to click a link or open an attachment. Simply previewing the email enabled the attackers to steal a username and password to gain access to the network, even though the email had been immediately deleted. The attackers were then able to create very convincing spear phishing emails to send to other university recipients, eventually leading to a breach of the university's human resources, finance and student administration databases.
- **Monash IVF.** In late 2019, Monash IVF, a national fertility business with clinics in six Australian states and territories, had its email server breached. Some of the breached emails are believed to have contained private personal information about patients in the email messages and attachments. The clinic's patients were also targeted with what appeared to be legitimate emails from the company but were, in fact, phishing scams. Notably, the company has been criticised by some patients about its handling of and response to the breach. Thus, in the long term, the most significant damage to the company may be the loss of trust and damage to its reputation.
- **Air New Zealand.** In July 2019, Air New Zealand voluntarily notified the New Zealand Privacy Commissioner that over 100,000 customers may have had their personal information – including names, email and mailing addresses, as well as a small number of limited passport details – compromised after two staff accounts were breached by phishing emails. Ironically, just two weeks earlier, the company had been commended by the Privacy Commissioner for its online customer Privacy Centre tool. Still, the company's rapid response, voluntary disclosure and customer notifications, and recognition of the need for good cultural training about email security, demonstrates a strong commitment to its customers and the right way to handle a security incident.
- **Landmark White.** In October 2019, the property valuations, personal details and driver's licences of 275,000 individuals were compromised and made available on the dark web. The breach is believed to have been perpetrated by an IT

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

contractor involving two data breaches of 170,000 datasets. The breach is estimated to have cost the company approximately $8 million.

- **P&N Bank.** During an upgrade of its third-party hosted and operated customer relationship management (CRM) system in December 2019, P&N Bank suffered a data breach that exposed detailed and sensitive financial information – including names, addresses, emails, phone numbers, ages and account balances – of an unspecified number of customers. This breach demonstrates the importance of ensuring security and privacy in third-party supplier and partner relationships.
- **Red Cross Blood Service.** In what has been described as Australia's largest data breach, in October 2016 the personal data of 550,000 blood donors was compromised when a contractor inadvertently posted a duplicate of the Red Cross member database on a website while doing experimental development work. The database included sensitive personal information such as names, gender, addresses, dates of birth and 'at-risk sexual behaviour'.

WARNING

The unauthorised use of company brands ('brandjacking') – which has been experienced by brands such as Australia Post, AGL and Optus – is a tactic used by bad actors to bait people into opening phishing emails and clicking malicious attachments or links to fraudulent sites. These sites can be used for financial gain, credential harvesting or simply wreaking havoc. You need to take back control of your brand by proactively identifying and working with law enforcement authorities to take out these sites because, although your organisation may have done nothing wrong, the backlash and damage to customer trust and brand reputation caused by a phishing attack will be yours.

The direct cost impacts associated with an attack or breach leading to disruption can include:

- Loss of business
- Loss of productivity
- Notification costs (including ongoing credit monitoring services for victims)

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Remediation and recovery costs
- Regulatory fines and penalties
- Legal costs

Indirect costs can be far more costly over the long term and may include:

- Brand reputation damage
- Customer churn due to loss of trust
- Competitive disadvantages

Brand reputation damage can be particularly devastating. For example, an organisation that is initially the victim of an attack can quickly become the villain. Retail organisations frequently end up in this dilemma as bad actors can then use sensitive customer information gained after the initial attack against the business to further target individual victims. The reputational damage is worse still for organisations that do not have an effective cybersecurity and cyber resilience strategy, which manifests itself as a poor detection and response capability. A delayed, inadequate or ineffective response can leave the general public with a general lack of faith in the organisation or, worse, concerns about dishonesty in the organisation's public handling of a breach.

Adhering to Compliance Requirements

Regulatory compliance requirements such as the European Union (EU) General Data Protection Regulation (GDPR), Australian Privacy Principles (APP) and New Zealand Privacy Bill, among others, place additional importance on cyber resilience for modern organisations around the world.

In addition to specific security and privacy requirements, many of these regulations typically include breach notification obligations that must be met in a timely manner (within 72 hours of breach detection in some cases). Therefore, it is important for organisations to have a robust cyber resilience program that ensures an

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

effective response and recovery effort, including required communications and notifications.

TIP

We discuss regulatory compliance requirements, including GDPR, APP, the New Zealand Privacy Bill and others, in Chapter 4.

Recognising the Cost of Downtime

For companies that rely on digital systems, any length of downtime can translate into a big loss of productivity, which is why cyber resilience is becoming so important. In some cases, downtime can even lead to loss of human life, such as in the case of an outage of critical systems in hospitals, air traffic control or hazardous areas.

According to the Ponemon Institute's *2019 Cost of a Data Breach Report*, the average total cost of a data breach is US $3.92 million. Direct costs associated with an outage caused by an attack can include lost revenues (which accounts for 36 per cent of the total damage according to the Ponemon Institute), legal fees and damages, regulatory fines, IT staff overtime and/or consulting fees, notification costs and long-term credit monitoring services for consumers (in some cases). The same NotPetya attack that hit DLA Piper (discussed earlier in this chapter) also targeted Danish shipping company Maersk and FedEx subsidiary TNT Express, with real damages estimated to be $378 million and $374 million (Australian dollar equivalent), respectively.

However, as demonstrated by several of the other attacks discussed earlier in this chapter, the long-term indirect cost of a breach – including loss of trust, brand reputation damage, loss of opportunities and loss of customers – can be far more devastating for an organisation. The Ponemon Institute found that abnormal customer turnover caused by breaches averaged 3.9 per cent in 2019.

REMEMBER

Your cyber resilience strategy, specifically how effectively your company prepares and responds to a breach – as in the case of Air New Zealand in contrast to Monash IVF – can make all the difference to how quickly your company recovers from the long-term damage caused by a potential breach.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Improving cybersecurity knowledge
- Getting your employees' attention
- Changing attitudes about cybersecurity

Chapter 3 Solving for Human Error

In the context of cybersecurity solutions, 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 each individual is different. In this chapter, you discover how to address all three components to truly move the needle on cybersecurity.

Lack of Knowledge about the Essentials of Cybersecurity

Knowledge is power – and when it comes to your employees, increasing knowledge is one of the most effective ways to reduce your cybersecurity risk. But effective doesn't have to mean boring. In fact, boring does the opposite of driving results – it causes your employees to switch off. Learning must also be persistent and non-intrusive if lasting, meaningful behavioural change is the goal.

REMEMBER

Human error is responsible for more than one-third (34 per cent) of all breaches according to the *Notifiable Data Breaches Statistics Report* from the Office of the Australian Information Commissioner (OAIC).

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Your employees are also very busy. If training is overly time-consuming, employees resent it 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' if it's going to work. Memories fade, the threat landscape changes, and employees lose that shared sense of responsibility for keeping the organisation safe. Therefore, security awareness training must continually communicate and reinforce key concepts and must be delivered regularly to every employee – for example, once a month. And those employees who need a little more help – based on test results and risk scoring – should receive targeted training as often as necessary.

TIP

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

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

- **Phishing.** Help people recognise possible phishing messages and show what can happen when they carelessly respond to one. According to research by PhishMe, the top reasons people fall for phishing emails include curiosity (13.7 per cent), fear (13.4 per cent) and urgency (13.2 per cent).
- **Ransomware.** Drive home how easy it is to get attacked – and how personally disastrous ransomware attacks can be.

TIP

- **Passwords.** Promote the use of strong passwords, such as passphrases, that are easy for employees to create – and make sure they never reuse personal passwords or write them down on a Post-It note 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. And a passphrase doesn't have to be a proper sentence or even be grammatically correct – so feel free to butcher the English language or any other language. It's your (or is it you're?) choice!
- **Data in motion.** Company data is especially vulnerable when it's in motion, and there are plenty of places it could go. You know this, but many employees don't.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Office hygiene.** Securing paper, desks, screens and buildings calls for a completely different kind of security awareness.
- **Physical security.** Physical security should not be forgotten; in fact, it's more important than it's ever been and has significant personal safety ramifications. 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). Random unknown and unsupervised intruders are not necessarily innocent visitors.
- **Sharing confidential work details in public.** Talking loudly or obliviously about important, confidential work information at the café or gym can mean other unwanted parties, such as competitors, could overhear you and act on that ill-gotten knowledge.

TECHNICAL STUFF

- **Vishing and SMS phishing ('SMSishing').** Vishing is the phone call equivalent of email phishing, and SMSishing is its evil text message cousin. Be sure your users understand these relatively new twists on the classic email phishing attack.
- **Privacy.** Show how to protect everybody's personal information: your company's, your customers', your partner's and your employees'.
- **General Data Protection Regulation (GDPR).** European Union GDPR compliance (Article 57) requires you to promote your employees' awareness and understanding of the risks, rules, safeguards, and their rights in relation to GDPR – and there can be severe penalties if you don't.
- **Payment Card Industry (PCI).** Help the company avoid social engineering attacks leading to financial loss and PCI non-compliance.

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.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Lack of Attention Leading to Failures in Cyber Awareness

The next challenge organisations must address to solve for human error is a general lack of attention by employees when it comes to applying cyber awareness knowledge in their day-to-day work. If all employees were always attending to security, protecting against cyber threats would be easier. But people are busy with other priorities.

To solve this problem, organisations need to attract their employees' attention and create an emotional connection that motivates the right action when it matters. In much the same way that many organisations have stressed the importance of safety in the workplace for decades, it's now time to stress the importance of security in the workplace. Employees understand that it is never okay to take shortcuts at the expense of safety. That same message needs to resonate with regard to security.

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 (meet Human Error and Sound Judgment at `www.mimecast.com/products/awareness-training/`), memes and recurring themes, jokes and sarcasm, and pop culture references.

WARNING

Humour can be extremely effective in getting your employees' attention, but don't overdo it. Too much humour can just as easily drown out your core message. Seriously.

TIP

Positive reinforcement is 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.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Lack of Concern: A Bad Attitude Towards Security

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 cybersecurity team. Perhaps there’s a stigma associated with IT security locking the user accounts of soon-to-be former employees, or a perception that if you’re getting a visit from IT security, you must’ve done something wrong. Inevitably, employees feel as though they are ‘in trouble’ if the security team is involved.

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.

WARNING

Unfortunately, in many cases, Australian CEOs aren’t earning top marks for their cybersecurity and cyber resilience strategies. Research by Vanson Bourne for Mimecast’s *2018 State of Email Security* report revealed that 44 per cent of respondents believed that their CEO was the weak link in their cybersecurity operation, and 51 per cent believed that their CEO would be unable to protect themselves from a direct attempt at a cyberattack.

Next, security teams must 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.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

STRIKING WHEN PEOPLE ARE AT THEIR MOST VULNERABLE

Bad actors have no moral compass, and their depravity can be quite disgusting when it comes to exploiting innocent victims. They will often launch attacks at times when people are stressed, distracted or otherwise in a hurry – which is 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'.

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, such as during the Australian bushfires of late 2019 and early 2020. Recent emails purporting to contain important health information and advice for your neighbourhood about the coronavirus have contained malicious links and attachments.

It's at these times that your employees are at the highest risk of making a mistake and becoming the next human error breach statistic.

TIP

Be particularly vigilant when you're in a hurry and most stressed. Take the time to carefully preview your emails before opening them, including verifying the sender (look at the actual email address, not just the friendly 'from' name), hovering over links rather than clicking on them (to see the actual website address without visiting the site), and considering if an attachment is safe to open (there's absolutely no reason that Australia Post or TNT can't send you the details of your shipment in the body of an email rather than a Word or PDF attachment). Few things will slow you down worse or stress you out more than falling victim to a phishing scam or infecting your office network with ransomware.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- » Establishing data governance
- » Exploring data protection solutions
- » Addressing compliance requirements
- » Implementing best practices

Chapter 4 Implementing Highly Effective Governance Structures

In this chapter you learn how data governance, data protection and compliance contribute to cyber resilience, and we provide some best practice recommendations for implementing your strategy.

Data Governance

With ever-growing volumes of data everywhere, increasingly stringent legal and regulatory requirements, broader individual privacy rights, and sophisticated emerging threats, the need for effective data governance in organisations has never been greater.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

A modern data governance strategy must address several key requirements, including:

- **Retention.** Your business records retention policy must meet legal and regulatory requirements, but it should also account for the business value of the information. Records that no longer have business value should be deleted as soon as legally permissible to lower storage costs, improve system performance, increase employee productivity and reduce potential liability.
- **Classification and labelling.** Organisations need to define an effective, and easy-to-understand and implement, classification and labelling taxonomy. This is particularly important in the wake of privacy regulations such as the European Union (EU) General Data Protection Regulation (GDPR), discussed later in this chapter, which requires organisations to respond to individual data subject access requests (DSARs) to identify, correct, delete and/or provide copies in a relatively short period of time.
- **Discoverability.** It's an unfortunate fact of life: we live in a litigious global society. Your data governance strategy needs to ensure you can comply with legal subpoenas and other requests in a timely, efficient, accurate and complete manner. A proactive approach to any investigation can help organisations limit the scope of discovery and the associated costs. Freedom of Information (FOI) requests are crippling many government entities, and responses are not meeting standards and requirements for timeliness because of the time and cost associated with discovery.
- **Employee productivity.** Your employees need to be able to work with your information – after all, that's the reason for having it in the first place! Your data governance strategy should ensure your employees can quickly and securely find, access and share the information they need, when they need it. You need to ensure a 'single version of the truth' (with versioning, deduplication and automated disposition) and 'security by default' (with at-rest encryption of sensitive information).

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Data Protection

Traditional data protection technologies and strategies were built for on-premises systems and typically include backup and recovery, as well as archiving. However, modern organisations need to revisit their approaches to data protection in today's cloud and mobile era.

Backup and recovery

Organisations moving their email services to the cloud often discover only after migrating that they need a separate solution to protect their data. Moreover, the drive to simplify IT has led growing numbers of organisations to revisit their data protection strategies for their on-premises email environments as well.

Exchange Online is part of Microsoft Office 365, which is the most popular Software-as-a-Service (SaaS) email application today. Yet, Office 365 offers no native email backup and recovery capability, and solutions designed for on-premises Exchange email systems tend to be costly and complex to manage. Organisations have long faced a difficult choice when it comes to backing up their critical email data:

- Back up to an on-premises infrastructure
- Deploy a cloud-based point solution
- Do nothing and hope for the best

Each of these options introduce disadvantages, inefficiencies and unacceptable risks to the organisation.

An integrated protection and archiving solution can help organisations:

- Simplify and automate email recovery
- Reduce cost and risk
- Enable email continuity and resilience

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

SUMMIT HOMES GROUP BUILDS ON MIMECAST EMAIL SECURITY AND ARCHIVING

An unexpected change in provider terms forced Summit Homes Group to rethink its entire email security, mailbox and archiving infrastructure. The Group, which builds around 1,000 homes each year in Western Australia, needed an unlimited mailbox solution that would accommodate constant changes in staff, as well as sending large attachments between the builders, clients and contractors.

The challenge

Operating in such a highly regulated industry, Summit Homes Group required a way to cost effectively store at least seven years' worth of email communications across hundreds of mailboxes. It also required a solution to integrate seamlessly with Microsoft Outlook and for users to be able to delete emails after they were read, knowing they could be easily accessed through an intuitive archive system at any time.

'As an industry we are required to have access to records for seven years,' said Fabio Fusari, Group IT Manager, Summit Homes Group. 'But as a company, we offer a lifetime warranty on our builds, so we need to hold onto our records for a lot longer in case there's a need to revisit a project.'

The solution

After an in-depth market assessment, Summit Homes Group selected Mimecast's M2A solution – one that integrates mailbox and archiving services with email security including email filtering and uniform resource locator (URL) rewriting.

Working with a local systems integrator, Summit Homes Group migrated in excess of five terabytes of mail archive data to Mimecast within a short period of time in the lead up to Christmas, one of the busiest times of year for the building industry.

Fusari explains the process of building a home from initial enquiry through to completion takes between one and three years, and there could be over 1,000 emails exchanged, including large attachments

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

such as plans, during that process. Compounding the challenge is the fact that sales consultants tend to move jobs quite frequently, so a conversation started between a buyer and the company could involve multiple salespeople.

Mimecast's archiving feature makes it easy for the company to go back and review all the email exchanges that occur in the lead up to a build period, as well as during and after the home has been completed.

'With the pressure of a looming contract end date, it was imperative that the transition ran smoothly and we were up and running in a relatively short period of time,' he said. 'Mimecast made it easy for us to access the mailbox of anyone that had left the company, and allowed us to extract the information and continue engagement with the customers seamlessly.'

Fusari sees Mimecast as the perfect fit for Summit Homes Group, with its similar culture and outlook, local presence and local data centres.

'The Mimecast solution is something that I don't have to think about too much, and for that reason it's great. It just works, and our only reason to contact the local support team is if new features are rolled out,' he said.

The benefits

Mimecast's solution for Summit Homes Group offers several benefits:

- It enables easy searchable access to terabytes of archived mailbox data.
- It provides integrated threat protection, archiving and continuity capability in one service.
- It seamlessly integrates with Microsoft Exchange and Office 365.
- It provides local support and data centre hosting.

Archiving

As email-borne threats evolve, it's more important than ever to have a separate and safe copy of your data. Once launched, threats can traverse a network quickly. If your archive is accessible to an attacker, a threat like ransomware can render it useless – and your business will suffer.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Archiving can be a powerful tool to help organisations address their data governance, data protection and compliance challenges, but traditional archiving is flawed. In fact, according to a Vanson Bourne global survey:

- **88 per cent** of organisations say they have experienced problems with their existing archiving solution
- Nearly **60 per cent** of organisations cite administrative complexity as a top challenge
- **56 per cent** of organisations are plagued by slow search performance
- **48 per cent** of organisations experience a lack of scalability

TECHNICAL STUFF

A modern cloud archive is a digital repository with multiple dimensions. It needs to:

- Safeguard corporate data
- Empower employees to access email when they want to and from anywhere
- Boost productivity and efficiency
- Ensure legal, regulatory and compliance obligations are fulfilled – fast

Compliance Laws

Regulatory compliance is non-negotiable: you are either in compliance or you are not, and nobody wants the latter. The breadth and scope of data security and privacy legislation that organisations in different industries must comply with continues to grow as governments respond to the increased threat of cybersecurity incidents by passing new laws. For any security incident, organisations must quickly determine what types of information may have been affected and which countries' laws might apply. An organisation may well have customers in multiple countries and may be subject to multiple sets of laws and jurisdictions with different requirements.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

The requirement for breach notifications is woven into many regulations and forms a critical aspect of compliance. Knowing who to notify – including customers, government agencies and regulators – and when they need to be notified, based on the type and severity of the breach, is fundamental in meeting your compliance obligations.

With growing exposure to legal and regulatory requirements, organisations need a cyber resilience strategy that meets best practice for compliance and legal risk mitigation. These regulations also mean that if you are the victim of a cyberattack and customer data is exposed, you may get hit with a significant fine, adding insult to injury. This makes having a cyber resilience strategy all the more important as it ensures data is protected and easily recoverable, and that you're able to quickly resume doing business as usual. Some examples of current compliance requirements around the world include:

- **Privacy laws**
  - **General Data Protection Regulation (GDPR) (European Union).** GDPR has quickly become the standard after which other privacy laws around the world are being modelled. GDPR requires businesses to implement data protection and privacy 'by design' and 'by default' to safeguard sensitive data about individuals residing in the EU. GDPR also applies to any organisation that does business with EU residents, regardless of where the organisation is actually located in the world.
  - **Privacy Act 1988 (Australia).** The Privacy Act 1988 establishes standards for collecting and handling personal information, referred to as the Australian Privacy Principles (APP). Under the Notifiable Data Breaches (NDB) scheme, organisations subject to the Privacy Act 1988 must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a serious data breach occurs.
  - **Privacy Bill (New Zealand).** The Privacy Bill is expected to become law in 2020. Under the proposed law, New Zealand businesses will be required to notify affected parties and the Office of the Privacy Commissioner of any serious privacy breaches. Overseas businesses, such as cloud service providers that work with New Zealand businesses, will also need to comply.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Data security laws**
  - **Australian Prudential Regulation Authority (APRA).** An independent statutory authority that supervises institutions across banking, insurance and superannuation and promotes financial system stability in Australia.
- **Data protection standards**
  - **Payment Card Industry (PCI) Data Security Standards (DSS).** PCI is not a legal mandate, but noncompliance can result in severe penalties and fines, as well as loss of card processing privileges. PCI is applicable to any organisation that transmits, stores or processes payment cards (such as credit and debit cards).

Best Practices

Going from being vulnerable to email-borne threats to being cyber resilient doesn't have to be time-consuming, expensive or painful. Step one is making cyber resilience planning a priority; it should be part of your organisation's foundation and business strategy. Next, have a firm understanding of your needs, strengths and weaknesses. Finally, consider every aspect of your business in your planning, and spread out the responsibility – even if it means layering in a third-party solution.

When you're ready to get started, follow these best practices to create an effective cyber resilience strategy for your organisation:

- **Security.** Security is your front-line defence, and a layered approach is key. Remember: Cybercriminals use email in a lot of different ways to execute attacks – even from within your organisation. This means you want an email security scanning layer that not only blocks spam and viruses, but also protects users from phishing, ransomware and impersonation fraud. Capabilities such as Uniform Resource Locator (URL) filtering, attachment sandboxing, instant preview and safe-file conversion of all incoming attachments are must-haves. Robust encryption and data loss prevention (DLP) technologies also help ensure sensitive data doesn't get into the wrong hands.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TIP

It's important to always stay one step ahead of attackers. One way to do this is through centralised monitoring, analysis and intelligence sharing to help better anticipate and defend against emerging tactics, techniques and procedures (TTPs). Plan to integrate your email security system and real-time threat intelligence feeds with third-party security information and event management (SIEM) systems to enable rapid threat correlation and analysis.

- **Data protection.** Email-borne threats, such as phishing and ransomware, can quickly spread across a network, so it's critical that organisations have a separate and secure copy of their data. If an attacker can get to your archive data, it can be destroyed or altered, and your business will suffer. Your archive should be immediate – with data captured in transit – as well as tamper-proof and perpetual. And users need the ability to sync files, folders, data and calendars – and recover them if an attack occurs. The bottom line: your business needs to function; end-users need the ability to find what they need when they need it; and you need fast search and e-discovery capabilities to meet regulatory compliance and governance requirements – no matter what. The only way to guarantee all of this is to create a central repository of corporate data that is permanently stored in a fully encrypted, immutable and redundant system.

TIP

Survey your employees to understand how they would like to access their data and historical emails. In many cases, accessibility can be improved, and the speed of archive retrieval can be increased.

- **Business continuity.** Email systems, whether hosted on-premises or in the cloud, can go down. Should downtime occur – whether due to a breach, human error or technical failure – you need to be prepared to quickly and seamlessly switch to an available service. Doing so should allow your employees to continue to work and access everyday tools, like Microsoft Outlook or G-Suite by Google Cloud, without disruption. Without company email, employees may resort to using personal email, which likely doesn't meet compliance requirements and could introduce significant business and security risk. But business continuity is about more than just email communication flow – access to email data is equally important.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TIP

To bolster your business continuity planning, implement a separate, always-on solution that provides multiple access systems through the web and mobile apps.

- **End-user empowerment.** Employees are your most valuable assets. Technology features can create a powerful human defence against email-borne threats – but employees need to understand how to use them, what to look for and how to respond. Regular and effective end-user training can help maximise your organisation's ability to respond to cyber threats. This helps make for a stronger, more productive workforce, while investing everyone more broadly with cyber resilience responsibility.

  TIP

  Intuitive interfaces, mobility, and integration with established apps also help to delegate responsibility more effectively, removing bottlenecks and freeing individuals to focus on value-added work.

- **Data breach response plan.** The Australian Privacy Commissioner advises that having a data breach response plan is the only realistic means by which organisations can effectively respond to cyber breaches in a manner that is efficient in terms of time and resources, reduces costs, and mitigates potential damage suffered by the organisation and other victims.

  TIP

  Test your response plan regularly by rehearsing a data breach scenario, including your communications plan for all impacted stakeholders, from employees to customers, investors, and potentially even the media. Consider hiring a breach coach (such as a lawyer) who can help guide you through your organisation's data breach communications and other response actions.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- **Know your risks and their impact on your business**
- **Create a human firewall and build a secure culture**
- **Be resilient by design and by default**
- **Incorporate the cloud in your cyber resilience plans**
- **Make regulatory compliance an ongoing priority**
- **Test plans and processes regularly and ensure a robust recovery capability**

Chapter 5 Ten Tips for Cyber Resilience

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

Identify Your Risks

The first step in developing a cyber resilience strategy for your organisation is knowing your risks. You need to identify:

- Which critical assets you are protecting
- What vulnerabilities exist in those assets
- What threats could exploit those vulnerabilities

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

With this information, you can then assess the risks each critical asset faces and plan your cyber resilience strategy accordingly.

Quantify the Impact of Disruption to Your Business

The average cost of IT disruptions – whether due to an attack, breach, outage or some other security incident – varies greatly across different businesses and industries. It’s important to understand exactly how disruptions to critical IT business systems – as well as supporting or dependent systems – impact your business. Armed with this information, you can appropriately prioritise your cyber resilience strategy for different systems according to their business value.

Train All Your Staff Frequently

Training your employees often helps reinforce consistent cybersecurity and cyber resilience messaging, and it enables you to keep your training modules short, sweet and memorable – which is definitely more effective than an annual 90-minute ‘death by PowerPoint’ presentation.

Create a Secure Culture

Emphasise the value of training (and lead by example, from the top of the organisation), reinforce positive cybersecurity and cyber resilience habits, and recognise the contributions of your staff to drive a secure culture throughout your organisation.

Architect Critical Systems for Resilience

Your critical systems (the ones you identified in the first two tips in this chapter) need to be designed for resilience. The European Union (EU) General Data Protection Regulation (GDPR) requires

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

organisations to ensure the security and privacy of sensitive data ‘by design’ and ‘by default’.

REMEMBER

Irrespective of the requirements of GDPR, this is a best practice to apply to your critical business systems – architect them to be resilient by design and by default.

Leverage the Cloud

In the past, business continuity and disaster recovery plans could be quite cost-prohibitive, requiring organisations to build ‘cold’ or ‘warm’ sites with redundant systems sitting idly waiting for a disaster or outage. IT teams would then be expected to restore the latest backups of data to these systems and get the business back up and running in a matter of days.

TIP

The public cloud makes real-time cyber resilience much more affordable and practical for any company. Leverage the cloud for high availability, replication and redundancy in your critical business systems. Ideally, you want your business to be back up and running in hours, if not immediately. Days of downtime means lost productivity, revenue and reputational damage.

Ensure Compliance is an Ongoing Activity

Sadly, compliance is not a ‘one and done’ activity. It’s also not the responsibility of a single department. Your entire organisation needs to be aware of relevant compliance requirements, and everyone needs to be responsible for achieving and maintaining compliance.

REMEMBER

New data security and privacy regulations are being passed and existing regulations are continually being updated and amended. Therefore, compliance must be an ongoing part of your cyber resilience strategy.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Test Business Continuity and Disaster Recovery Plans

Ensure business continuity and disaster recovery plans are regularly reviewed and maintained, then test them – frequently. Tests should incorporate various techniques, including read-through (or checklist) tests, structured walkthrough (or tabletop) tests, simulation tests, parallel tests and full interruption (or cutover) tests.

Design, Document and Test Your Cyber Resilience Processes

Along with your business continuity and disaster recovery plans, you need to ensure that the cyber resilience capabilities in your critical systems (and dependent or supporting systems) are well documented and regularly tested. This must also include your crisis communications across all impacted stakeholders.

Recover from a Cyber Breach

The Ponemon Institute reports that the breach lifecycle (the time between when a breach occurs to when it is contained) is 279 days. The faster a breach can be identified and contained, the lower the costs associated with the breach. Of course, once you've contained a breach, you need to recover and restore systems, applications, data, and normal business operations. This is an often-overlooked impact of data breach incidents. The Ponemon Institute reports that significant data breach costs can continue to impact an organisation for several years after a breach. This fact speaks directly to the need for fast and effective response and recovery capabilities in your cyber resilience strategy.

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Email Security 3.0 is more than a secure email gateway

Achieve comprehensive protection with a pervasive, multi-zoned, integrated email security strategy.

Learn more at www.mimecast.com/emailsecurity3.0

© 2020 Wiley Publishing Australia Pty Ltd. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Build cyber resilience across your organisation

Disruption is today's villain, and in an increasingly digitally interconnected world the impact of cybercrime, tech failure and even human error can not only impact your business and your customers, but also society as a whole.

Cyber resilience helps you defend your business from cyberattack by minimising the impact of disruptions and keeping your business running as smoothly as possible during recovery. This book introduces you to the key elements of an effective cybersecurity and cyber resilience strategy.

Inside…

- Understand why you need to be both cybersecure and cyber resilient
- Prepare to respond to cyber threats
- Defend your organisation from phishing and ransomware
- Reduce the impact of cyber disruptions
- Train your team to stay cyber aware
- Protect your reputation from cyber attackers

mimecast®

Lawrence Miller has worked in information technology for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 180 *For Dummies* books on technology and security topics. **Daniel McDermott** is a 20+ year cyber veteran and editor of the local blog and podcast series GetCyberResilient.com.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-0-730-38412-0
Not For Resale

9 780730 384120

for dummies®
A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.