packt

1ST EDITION

A CISO Guide to Cyber Resilience

A how-to guide for every CISO to build a resilient security program

DEBRA BAKER

Foreword by Ray Rothrock, Former CEO, RedSeal, Author - Digital Resilience (2018)

A CISO Guide to Cyber Resilience

A how-to guide for every CISO to build a resilient security program

Debra Baker

‹packt›

A CISO Guide to Cyber Resilience

Group Product Manager: Pavan Ramchandani
Publishing Product Manager: Prachi Sawant
Book Project Manager: Ashwin Kharwa
Senior Editor: Divya Vijayan
Technical Editor: Arjun Varma
Copy Editor: Safis Editing
Proofreader: Divya Vijayan
Indexer: Tejal Daruwale Soni
Production Designer: Prafulla Nikalje
Senior DevRel Marketing Executive: Linda Pearlson
DevRel Marketing Coordinator: Marylou De Mello

First published: April 2024
Production reference: 1050424

Published by Packt Publishing Ltd.
Grosvenor House
11 St Paul's Square
Birmingham
B3 1RB, UK.

ISBN 978-1-83546-692-6
www.packtpub.com

To my parents, who always kept me on the right path and taught me the value of hard work and ethics. To my husband, Bill – I would not have been able to write this book without his love and support. To my children, who are always cheering me on.

– Debra Baker

Foreword

While CEO of RedSeal, Inc. in San Jose, California, I had the privilege of working with Debra Baker. RedSeal, a cyber security analytics company, had a robust business assessing the network risks of enterprises. Our many customers included large Fortune 500 companies as well as many US Government civilian agencies, branches of the armed services, and the IC. During this time, in the late 201X's, ransomware evolved to be the #1 attack on companies. It seems the bad guys had indeed found where the money was, and that was in ransoming data. Debra came to RedSeal with a mission in mind, and that mission was to secure the nation.

Debra has a wealth of knowledge, practical real-world experience, much hearty advice, and most importantly, a great way of communicating all that to me, to RedSeal, and to our customers. She rocks when it comes to certifications, of which there are too many to list. She was a sought-after expert in the RedSeal world. Ultimately, Debra was selected as one of the 10 Most Eminent Women Leaders in Security (2021), successfully completed several management programs with an emphasis on cybersecurity, and was eventually named among the "Top 100 Women in Cybersecurity." She, simply put, is one to be reckoned with if you are a cyber bad guy.

Cyber is ever-changing. Attacks are increasing in number and complexity. Their success rate is enough to still make the news. And the skills required to defend an organization remain scarce. To be able to discuss, understand, and ask the right questions in order to trust your cyber team and leadership is essential. Debra brings all that home in a way we all can understand. So, it was no surprise when she reached out to me about her book, *A CISO Guide to Cyber Resilience*. It made perfect sense that she, of all people, should share her experiences with us all through the printed word. If I had to commission someone to write such a book, Debra would be my first call.

A CISO Guide to Cyber Resilience is both a strategy and a tactics knowledge set. A former CISO herself, she gets the power of a policy and the intricacies of implementing it. She lays out in plain management English how to think about the data in your organization and how to protect it. She talks clearly about unencrypted data, phishing, malware, third-party vendor compromise, software vulnerabilities, unintended misconfigurations, and the many other things that contribute to an organization's vulnerability.

Cyber vulnerability is here to stay. Therefore, Debra's book, *A CISO Guide to Cyber Resilience*, is an invaluable resource for you, tattered corners and all. I highly recommend it to all managers of any organization.

Ray Rothrock
Former CEO, RedSeal
Author, Digital Resilience (2018)
Feb 7, 2024

Contributors

About the author

Debra Baker is a cybersecurity expert with over 30 years of experience. She began her career in the U.S. Air Force and has worked at IBM, Cisco, and Entrust DataCard. As President of TrustedCISO, she specializes in strategic cybersecurity, risk management, and compliance advisory services, helping clients navigate complex frameworks such as NIST, SOC2, ISO27001, FedRAMP, and StateRAMP. A CISSP and CCSP holder, Debra has a provisional patent for an AI-driven vendor assessment tool and founded Crypto Done Right. She's recognized as one of the top 100 Women in Cybersecurity.

About the reviewer

Jean-Luc Dupont is a seasoned Chief Information Security Officer with a proven track record in strengthening global corporations, especially in highly regulated industries. With over 25 years of experience in cybersecurity, he has served as a CISO for companies such as Kestra, American Credit Acceptance, IDEMIA, and Oberthur. He holds a Bachelor of Science in applied computing from Newcastle Polytechnic (UK) and a Master of Science from EPITA (France). His passion for cybersecurity extends beyond his professional duties to side projects such as Security Rabbits, a daily security digest, and his book *Secur-What?! Learning Cybersecurity from Mistakes*, Independently published.

Alex Bazay is the CISO of Align, a leading provider of cloud-based IT solutions for the financial industry. He oversees the security strategy, operations, and governance of the company's global network and data. Alex boasts over 25 years of experience in designing, implementing, and managing intricate IT infrastructures and security systems for hedge funds and asset managers, with multiple certifications in information systems auditing and security.

Alex excels in insider threat detection, network security, risk management, data center, and vulnerability management. He is passionate about protecting the integrity, confidentiality, and availability of his clients' data and assets and ensuring compliance with industry standards and regulations. Collaborating with a skilled and diverse team of security professionals, he partners with internal and external stakeholders to deliver innovative and effective solutions that address the evolving needs and challenges of the financial sector.

Table of Contents

Security Policies

Security and Risk Management

Securing Your Endpoints

Data Safeguarding

7

Security Awareness Culture

8

Vulnerability Management

11

Taking Your Endpoint Security to the Next Level

12

Secure Configuration Baseline

13

Classify Your Data and Assets

Preface

Greetings, fellow cybersecurity enthusiasts! Welcome to the world of cyber resilience, where the goal is to build a security program that enables your organization to not only withstand cyber-attacks but also to recover swiftly. As the United States Department of Homeland Security aptly defines it, cyber resiliency is the "*ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions*."[1] It's not just a process; it's an ultimate state of readiness. An organization achieves resilience when it can bounce back from any disruption, be it a ransomware attack or any other cyber threat, without major disruptions.

In today's landscape, cyber-attacks are becoming increasingly sophisticated and prevalent. In the book *Big Breaches*[2], it is highlighted that the root causes of nearly every data breach can be traced to six key factors:

- Unencrypted data
- Phishing attacks
- Malware
- Third-party vendor compromise
- Software vulnerabilities
- Unintended misconfigurations

In this book, we will explore practical safeguards that you can implement immediately to defend against these root causes of data breaches. These safeguards will not only enhance your information security program but also make it cyber-resilient, ready to face the latest threats. We'll delve into some of the most significant cyber-attacks in recent history and discuss what could have been done to prevent or mitigate their impact. Most importantly, this book will guide you on how to transform your network into a cyber-resilient fortress, ensuring your organization's ability to recover swiftly from any cyber-attack.

This book takes you on a journey, partly fictional, where you'll witness a catastrophic cyber attack on BigCo and see how Megan, the **Chief Information Security Officer** (**CISO**), responds decisively. Megan's actions will stop the attack, initiate responses, and put measures in place to prevent future attacks. As the saying goes, it's not a matter of *if* your company will be cyber-attacked, but *when*. *Chapters 1* to *10* will provide you with foundational tools to prepare for and respond to cyber-attacks.

1 (Schwien and Jamison)

2 (Daswani, 15)

Chapters 11 to *14* will elevate your company's IT security program to the next level of cyber resilience. You'll find step-by-step guidance on implementing the necessary safeguards in your security program, whether your organization is small, medium, or large. Each chapter focuses on a specific safeguard, and the good news is that the steps you'll learn here not only form the foundation of cyber defense but also assist your organization in meeting various compliance frameworks, standards, and laws while becoming cyber-resilient.

Who this book is for

This book is for CISOs, directors of information security, aspiring CISOs, and cybersecurity professionals at all levels who want to learn how to build a resilient security program. Cybersecurity professionals will uncover valuable insights for enhancing their strategic and operational roles. This book is crafted to serve the following key personas in the cybersecurity field:

- **Cybersecurity leaders and CISOs**: As a leader in cybersecurity, you are continuously navigating the evolving threat landscape. You have to balance organizational needs with the budget while defending from the latest threats. This book provides strategies to elevate your leadership by developing and implementing a comprehensive cyber-resilient information security program.
- **Cybersecurity practitioners**: Whether you are delving into the cybersecurity arena or looking to deepen your existing expertise, this guide offers a wealth of practical knowledge. From important safeguards to effective risk management techniques, you will gain skills to understand a more holistic view of cybersecurity as well as fortify your role and progress in your career trajectory.
- **IT professionals and support staff**: Often the first line of defense in an organization, your role is crucial in maintaining cyber hygiene and resilience. This book equips you with an understanding of common and emerging threats, as well as best practices in response and recovery procedures. Enhance your capabilities in supporting cybersecurity initiatives and excel in roles focused on maintaining organizational cybersecurity.

Each chapter of the *CISO Guide to Cyber Resilience* includes real-world examples, actionable recommendations, and distilled wisdom from my extensive experience in the field. This book is more than a guide; it's a companion in your journey toward mastering cyber resilience.

What this book covers

Chapter 1, *The Attack on BigCo*, explains a ransomware attack on a fictional company, what worked to limit the damage, and how they recovered. It explains what ransomware is, how it can bring down a network, and how to recover.

Chapter 2, *Identity and Access Management*, explains that 99.99% of account attacks can be prevented by using **two-factor authentication** (**2FA**). It also includes a discussion on methods to use for 2FA and password managers, as well as how NIST 160-3 can be successfully utilized.

Chapter 3, *Security Policies*, explains that security policies are foundational to guide your organization's security program. It covers how your security policies meet laws and regulations, and the importance of due diligence.

Chapter 4, *Security and Risk Management*, explains that security and risk management is the process of balancing cyber risks, the controls to thwart attacks, and the budget. Business is about making money. Security and risk management is the process of choosing the controls that work for your company's budget. Your company can't be 100% secure, nor can there be 0% risk. Security is a balance of what is most important, what can wait, and what risks are acceptable to your business.

Chapter 5, *Secure Your Endpoints*, talks about securing your endpoints. At a very basic level, you need an antivirus. Endpoint security has evolved. For getting the basics down, we'll talk about antivirus and anti-malware. In addition, we will discuss testing your home firewall to ensure it is configured properly.

Chapter 6, *Data Safeguarding*, explains that good backups are critical. More importantly, ensuring *offline* backups is paramount to secure your company's data. We will be discussing the importance of testing backups, leveraging the cloud, and business continuity.

Chapter 7, *Security Awareness Culture*, explains the importance of developing a security awareness culture. No matter what tools and security controls you have deployed, you still need security awareness training for everyone in your company.

Chapter 8, *Vulnerability Management*, explains the importance of vulnerability scanning and patching security vulnerabilities. If you stay up to date with the latest threats, you will understand that it's not easy to keep up with patching all those thousands of vulnerabilities. We'll be discussing practical strategies to prioritize vulnerability patching, as well as ensuring your source code is secure.

Chapter 9, *Asset Inventory*, explains the importance of creating an asset inventory. To know what to protect, you have to understand what assets you have, whether they are software, hardware, or ephemeral. An asset inventory is foundational in a cyber-resilient organization. We'll also discuss mobile device management and knowing your network.

Chapter 10, *Data Protection*, explains the importance of encrypting your company's data, whether in transit or at rest. The reason is that if an attacker can gain access to your network or even steal an employee's laptop, if the data is encrypted, then the data is protected. The most amazing part is that there is no breach if the data stolen is encrypted.

Chapter 11, *Taking Your Endpoint Security to the Next Level*, explains the importance of moving past the basics and into more advanced safeguards. The latest antivirus is called **Endpoint Detection and Response** (**EDR**). It takes the traditional antivirus to the next level. Some even include 24/7 helpdesk support, also known as **Managed Detection Response** (**MDR**). We'll also demystify **Extended Detection Response** (**XDR**), **Cloud Security Posture Management** (**CSPM**), and the **Cloud Native Application Protection Program** (**CNAPP**).

Chapter 12, *Secure Configuration Baseline*, explains the importance of creating a security baseline. Essentially, this is a configuration that is applied across devices, hosts, and the cloud. For the commercial space, the **Center for Internet Security** (**CIS**) is typically used, whereas for the federal government, it's STIGS.

Chapter 13, *Classify Your Data and Assets*, explains the importance of classifying your data and assets. A fully developed, mature, advanced information security program has an asset inventory and has classified those specific assets with sensitive data as critical.

Chapter 14, *Cyber Resilience in the Age of Artificial Intelligence (AI)*, explains the importance of cyber resilience in the age of AI. With the rush to use and deploy AI, there are new cybersecurity concerns such as data leakage, use of AI by hackers, and bias in AI. This chapter will discuss responsible AI and measures to take to ensure your company deploys AI in a safe manner.

To get the most out of this book

It is good to have a basic understanding of information security and the cloud before reading this book. I will explain each concept and each chapter builds on the previous, providing a roadmap of how to build a resilient cybersecurity program.

Download templates and the roadmap to cyber resilience

You can download the following templates and my roadmap to cyber resilience from my TrustedCISO website (`https://trustedciso.com/e-landing-page/ciso-guide-to-cyber-resilience/`):

- *CISO Guide to Cyber Resilience*
- Software evaluation template
- Encryption template

Conventions used

There are a number of text conventions used throughout this book.

Bold: Indicates an important word(s), command, topic, or title. For example, words that need to be taken into consideration such as this example: ">**nslookup google.com**"

Italics: emphasizing an important word or topic. An example is "This is a big caution. I can't recommend *not* using a complex password."

> **Tips or important notes**
> Appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, mention the book title in the subject of your message and email us at `customercare@packtpub.com`.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit `www.packtpub.com/support/errata`, select your book, click on the Errata Submission Form link, and enter the details.

Piracy: If you come across any illegal copies of our works in any form on the Internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `authors.packtpub.com`.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions, we at Packt can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about Packt, please visit `packtpub.com`.

Share Your Thoughts

Once you've read *A CISO Guide to Cyber Resilience*, we'd love to hear your thoughts! Please click here to go straight to the Amazon review page for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Download a free PDF copy of this book

Thanks for purchasing this book!

Do you like to read on the go but are unable to carry your print books everywhere?

Is your e-book purchase not compatible with the device of your choice?

Don't worry!, Now with every Packt book, you get a DRM-free PDF version of that book at no cost.

Read anywhere, any place, on any device. Search, copy, and paste code from your favorite technical books directly into your application.

The perks don't stop there, you can get exclusive access to discounts, newsletters, and great free content in your inbox daily

Follow these simple steps to get the benefits:

1. Scan the QR code or visit the following link:

`https://packt.link/free-ebook/9781835466926`

2. Submit your proof of purchase.
3. That's it! We'll send your free PDF and other benefits to your email directly.

Part 1: Attack on BigCo

In this part, you will follow a fictional company called *BigCo* as it undergoes a ransomware attack. You'll get to see firsthand how Megan, BigCo's CISO, leads the company through the attack and how it recovers. You'll learn how to limit the damage caused by these kinds of attacks, mastering what ransomware is and how it can take down a network. Most importantly, you'll see how to prepare for and recover from a ransomware attack.

This section contains the following chapter:

- *Chapter 1*, *The Attack on BigCo*

1
The Attack on BigCo

This chapter is fictional and based on a horrendous cyber-attack on BigCo and how Megan, the **Chief Information Security Officer** (**CISO**), responds. Megan will decisively stop, respond, and put measures into place that will help prevent another attack. As the saying goes, it's not if your company will be cyber-attacked; it's when. By the end of this chapter, you will understand how the hackers gained access to BigCo's network, how the ransomware was deployed, and the measures that were taken in order to make the network resilient.

In this chapter, we're going to cover the following main topics:

- BigCo – the attack
- BigCo – cross-team co-ordination
- BigCo – recovery
- BigCo – the anatomy of a ransomware attack

BigCo – the attack

Megan, the **Chief Information Security Officer** (**CISO**) of a multi-national corporation, gets the call at 3:00 AM about major sections of her company BigCo's network being down. The CISO is responsible for the cybersecurity of the company, ensuring compliance, risk management, and sufficient defenses are in place. It's the highest-level position in cybersecurity. It can be at the Director level, Vice President, or directly under the CEO, depending on the importance of cybersecurity within an organization. Megan is a Director of Information Security at BigCo with the title of CISO, and she reports to the **Chief Information Officer** (**CIO**). Typically, the CIO will exist over the information technology and information security departments. In this case, Megan reports to the CIO, Mark.

Megan knows getting a call at 3:00 AM means this outage must be bad because she typically wouldn't be called in the middle of the night for a typical network outage. First, she quietly gets up so as not to wake her partner. She goes to her home office and calls Mark, the CIO of BigCo. Megan says, "Mark, hi. What happened?" Mark replies, "Well, from what we can tell, it wasn't a bogus email link like last time." "The new security awareness program you introduced is working as well as the email phishing