



# A CISO Guide to Cyber Resilience : A How-To Guide for Every CISO to Build a Resilient Security Program

Baker, Debra

Monografía

Explore expert strategies to master cyber resilience as a CISO, ensuring your organization's security program stands strong against evolving threats

**Key Features**

- Unlock expert insights into building robust cybersecurity programs
- Benefit from guidance tailored to CISOs and establish resilient security and compliance programs
- Stay ahead with the latest advancements in cyber defense and risk management including AI integration

**Purchase of the print or Kindle book includes a free PDF eBook**

**Book Description**

The rising number of cybersecurity attacks is a top concern for organizations across the globe. Amid the ever-evolving cybersecurity landscape, CISOs play a crucial role in fortifying organizational defenses and safeguarding sensitive data. Written by the CEO of TrustedCISO, with 30+ years of experience, A CISO Guide to Cyber Resilience will take you through some of the latest and most significant large-scale cyber-attacks and guide you on how to make your network cyber-resilient so your company can quickly recover from any attack. You'll begin with an in-depth analysis of a ransomware attack targeting a fictional company, BigCo, understanding its impact and response strategies, and then delve into fundamental security policies and controls. As you progress, you'll find that every chapter provides actionable skills and insights suitable for various levels of expertise, from basic to intermediate. Toward the end, you'll explore advanced concepts such as zero-trust, managed detection and response, security baselines, data and asset classification, and the integration of artificial intelligence and cybersecurity. By the end of this book, you'll be equipped with the knowledge and skills necessary to build, manage, and improve a resilient cybersecurity program, ensuring your organization remains protected against evolving threats. What you will learn

- Defend against cybersecurity attacks and expedite the recovery process
- Protect your network from ransomware and phishing
- Understand products required to lower cyber risk
- Establish and maintain vital offline backups for ransomware recovery
- Understand the importance of regular patching and vulnerability prioritization
- Set up security awareness training
- Create and integrate security policies into organizational processes

**Who this book is for**

This book is for new CISOs, directors of cybersecurity, directors of information security, aspiring CISOs, and individuals who want to learn how to build a resilient cybersecurity program. A basic understanding of cybersecurity concepts is required

<https://rebiunoda.pro.baratznet.cloud:28443/OpacDiscovery/public/catalog/detail/b2FpOmNlbGVicmF0aW9uOmVzLmJhcmF0ei5yZW4vMzU1NzIzMzU>

**Título:** A CISO Guide to Cyber Resilience A How-To Guide for Every CISO to Build a Resilient Security Program

**Edición:** 1st ed

**Descripción física:** 1 online resource (239 pages)

**Contenido:** Cover -- Title Page -- Copyright and Credits -- Foreword -- Contributors -- Table of Contents -- Preface -- Part 1: Attack on BigCo -- Chapter 1: The Attack on BigCo -- BigCo - the attack -- BigCo - cross-team co-ordination -- BigCo - recovery -- BigCo - the anatomy of an attack -- Summary -- Part 2: Security Resilience: Getting the Basics Down -- Chapter 2: Identity and Access Management -- Two-factor authentication and why you need it -- Something you know -- Something you are -- Something you have -- Password complexity and NIST 800-63-3B -- Application security -- Password manager -- Quick reference -- Summary -- Chapter 3: Security Policies -- Where are your policies, and are they being used? -- Compliance begins with laws and regulations -- Nortel hack -- Importance of Due diligence -- Summary -- Chapter 4: Security and Risk Management -- What is risk management? -- Identifying risks -- Risk assessment -- Monitoring your controls -- Key performance indicators (KPIs) -- Quick reference -- Summary -- Chapter 5: Securing Your Endpoints -- Antivirus/anti-malware -- Virtual private network (VPN) -- What is phishing? -- Moving to remote work -- LastPass hack -- Testing your home firewall -- Network access control (NAC) and Zero Trust -- Application firewall -- Mirai botnet -- Securing your browser -- Turning on your application firewall -- Okta hack -- Quick reference for endpoint security -- Summary -- Chapter 6: Data Safeguarding -- Offline backups -- Testing your backups -- Cryptographic hashing -- Availability in the cloud -- Business continuity -- Recovery time objective (RTO) -- Recovery point objective (RPO) -- Maximum tolerable downtime (MTD) -- Succession planning -- AWS DDOS attack -- Disaster recovery -- Redundancy in architecture -- Disaster recovery roles and responsibilities -- Testing disaster recovery -- Summary -- Chapter 7: Security Awareness Culture -- Security awareness training is foundational -- Security is everyone's responsibility -- Materiality assessment -- Disclosure requirements -- Governance and management -- Third-party involvement -- Security awareness training is mandatory and tracked -- Chapter 8: Vulnerability Management -- What are software vulnerabilities? -- Common Vulnerabilities and Exposures -- What is the NIST definition of software vulnerabilities? -- CVSS -- Common Weakness Enumeration -- Known Exploited Vulnerabilities -- CVE, CWE, and KEV -- What we're up against -- Prioritizing your remediations -- CISA's KEV Catalog -- CVSS metric - Attack Vector -- CVSS metric - Attack Complexity -- CVSS metric - Privileges Required -- CVE priority -- Starting with vulnerability scans -- Making it fun -- In the cloud -- Securing your code -- IaC -- SAST -- DAST -- IAST -- Software composition analysis -- OWASP -- Summary -- Chapter 9: Asset Inventory -- Asset inventory -- Identifying your assets -- What is the NIST definition of asset inventory? -- Automating your asset inventory -- Change management -- NIST security-focused change management -- Phase 1 - Planning -- Phase 2 - Identifying and implementing configurations -- Phase 3 - Controlling configuration changes -- Phase 4 - Monitoring -- Mobile device management (MDM) -- Knowing your network -- Quick reference for asset management -- Summary -- Chapter 10: Data Protection -- Encrypt your data! -- Introduction to encryption -- History of encryption -- Encryption basics -- Encrypted data means there is no breach! -- What is PII? It depends... -- NIST's definition of PII -- Third-party risk management -- SolarWinds attack -- Vendor management policy -- Vendor management contract clauses -- Critical vendors -- Train your staff -- Vendor risk rating -- Data loss protection Insider threats - the hidden danger -- Quick reference for data protection -- Summary -- Part 3: Security Resilience: Taking Your Security Program to the Next Level -- Chapter 11: Taking Your Endpoint Security to the Next Level -- Endpoint detection and response (EDR) - Focusing on the "R" -- Managed detection and response (MDR) -- Extended detection and response (XDR) -- SOAR -- Cloud security posture management (CSPM)/Cloud-native application protection program (CNAPP) -- What is CSPM/CNAPP? -- Zero trust vs. software-defined perimeter -- How a typical TLS session works -- What is mutual authentication? -- DNS protection -- What do DNS protections provide? -- Quick reference for zero trust -- Summary -- Chapter 12: Secure Configuration Baseline -- Security baseline -- What compliance does your company have to meet? -- System and Organizational Controls (SOC) 2 -- International Standard Organization (ISO) 27001 -- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) -- Cybersecurity Maturity Model Certification (CMMC) -- NIST 800-171 vs. CMMC -- SOC 1 -- Sarbanes-Oxley Act (SOX) -- Payment Card Industry Data Security Standard (PCI-DSS) -- Health Insurance Portability and Accountability Act (HIPAA) -- Health Information Technology for Economic and Clinical Health (HITECH) -- HITRUST -- NIST 800-53 - One framework to rule them all -- Creating your security baseline -- Quick reference for creating a security baseline -- Summary -- Chapter 13: Classify Your Data and Assets -- Start with your data -- Shared Responsibility Model -- Classifying your assets -- Monitoring -- Subnetting -- Segmentation -- Sony hack -- Quick reference for securing critical assets -- Summary -- Chapter 14: Cyber

Resilience in the Age of Artificial Intelligence (AI) -- ChatGPT -- Securing ChatGPT -- What can go wrong with ChatGPT? Artificial intelligence (AI) -- Machine learning (ML) -- Natural language processing (NLP) -- Deep learning (DL) -- Generative AI (Gen AI) -- What is responsible AI? -- EU AI Act -- Secure AI framework (SAIF) -- AI and cybersecurity - The good, the bad, and the ugly -- The good -- The bad -- The ugly -- AI bias -- Systematic bias -- Statistical bias -- Human bias -- NIST AI RMF -- Summary -- Index -- Other Books You May Enjoy

**ISBN:** 1-83546-103-4

**Materia:** Computer security Business enterprises- Computer networks- Security measures

**Autores:** Rothrock, Ray

**Enlace a formato físico adicional:** 1-83546-692-3

---

### **Baratz Innovación Documental**

- Gran Vía, 59 28013 Madrid
- (+34) 91 456 03 60
- [informa@baratz.es](mailto:informa@baratz.es)