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

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

Edición: 1st ed

Editorial: Birmingham Packt Publishing, Limited 2024 2024

Descripción física: 1 online resource (239 pages)

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