Cyber Security The Mitigation Strategies

Cybersecurity and Secure Information Systems
Confronting Cyber Risk
Challenges and Solutions in Smart Environments
Network Security Strategies
Protect your network and enterprise against advanced cybersecurity attacks and threats
Risks and Mitigation
Department of Homeland Security Appropriations for 2012
Hacking Techniques Used to Interfere the U.S. Election and to Exploit Government & Private Sectors, Recommended Mitigation Strategies and International Cyber-Conflict Law
Cyber-Security Threats, Actors, and Dynamic Mitigation
Issues Surrounding the Cyber Security of the Electricity Infraestructure and Associated Mitigation Strategies
Cyber Security Enhancement Against Cyber-attacks on Microgrid Controllers
Emerging Attacks and Mitigation Strategies
Understanding Cybersecurity Management in FinTech
Challenges, Strategies, and Trends
High Schools, Undergraduate, Graduate and Post-Graduate Studies.
Cybersecurity Threats with New Perspectives
Human Dimensions of Cybersecurity
Hearings Before a Subcommittee of the Committee on Appropriations, House of Representatives, One Hundred Twelfth Congress, First Session
Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks
Cyber Security And Supply Chain Management: Risks, Challenges, And Solutions
Equity of Cybersecurity in the Education System
Modern Theories and Practices for Cyber Ethics and Security Compliance
Managing Information Security Risk: Organization, Mission, and Information System View
Cyber-Security Threats, Actors, and Dynamic Mitigation
Metrics and Methods for Security Risk Management
Strategic Information Security
Detecting and Mitigating Robotic Cyber Security Risks
Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies
An Embedded Endurance Strategy for Cybersecurity
Enterprise Cybersecurity
Data Privacy and Cybersecurity Law
Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization
6th International Conference, ATIS 2016, Cairns, QLD, Australia, October 26-28, 2016, Proceedings
Routledge Companion to Global Cyber-Security Strategy
Threat Hunting in the Cloud
Mitigate exploits, malware, phishing, and other social engineering attacks
Optimal Spending on Cybersecurity Measures
Cybersecurity Threats, Malware Trends, and Strategies
Applications and Techniques in Information Security

LACEY JUSTICE

Cybersecurity and Secure Information Systems BoD – Books on Demand
Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.
Confronting Cyber Risk Syngress
Implement a vendor-neutral and multi-cloud cybersecurity and risk mitigation framework with advice from seasoned threat hunting pros In Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks, celebrated cybersecurity professionals and authors Chris Peiris, Binil Pillai, and Abbas Kudrati leverage their decades of experience building large scale cyber fusion centers to deliver the ideal threat hunting resource for both business and technical audiences. You'll find insightful analyses of cloud platform security tools and, using the industry leading MITRE ATT&CK framework, discussions of the most common threat vectors. You'll discover how to build a side-by-side cybersecurity fusion center on both Microsoft Azure and Amazon Web Services and deliver a multi-cloud strategy for enterprise customers. And you will find out how to create a vendor-neutral environment with rapid disaster recovery capability for maximum risk mitigation. With this book you'll learn: Key business and technical drivers of cybersecurity threat hunting frameworks in today's technological environment Metrics available to assess threat hunting effectiveness regardless of an organization's size How threat

hunting works with vendor-specific single cloud security offerings and on multi-cloud implementations A detailed analysis of key threat vectors such as email phishing, ransomware and nation state attacks Comprehensive AWS and Azure "how to" solutions through the lens of MITRE Threat Hunting Framework Tactics, Techniques and Procedures (TTPs) Azure and AWS risk mitigation strategies to combat key TTPs such as privilege escalation, credential theft, lateral movement, defend against command & control systems, and prevent data exfiltration Tools available on both the Azure and AWS cloud platforms which provide automated responses to attacks, and orchestrate preventative measures and recovery strategies Many critical components for successful adoption of multi-cloud threat hunting framework such as Threat Hunting Maturity Model, Zero Trust Computing, Human Elements of Threat Hunting, Integration of Threat Hunting with Security Operation Centers (SOCs) and Cyber Fusion Centers The Future of Threat Hunting with the advances in Artificial Intelligence, Machine Learning, Quantum Computing and the proliferation of IoT devices. Perfect for technical executives (i.e., CTO, CISO), technical managers, architects, system admins and consultants with hands-on responsibility for cloud platforms, Threat Hunting in the Cloud is also an indispensable guide for business executives (i.e., CFO, COO CEO, board members) and managers who need to understand their organization's cybersecurity risk framework and mitigation strategy.

Challenges and Solutions in Smart Environments Academic Conferences Limited

"Microgrids are constantly evolving to integrate more renewable generation, operate autonomously, provide continuous power supply to critical and high-value loads and offer advanced control capabilities necessitating the deployment of a communication infrastructure vulnerable to cyber intrusions. This thesis provides a cyber security analysis of microgrid systems and proposes novel cyber resilient control strategies to mitigate cyber-attacks. Benchmark systems are first developed to provide a basis for the cyber security analysis of diverse microgrid configurations operating based on different control strategies. Interest is attributed to cyber-attacks compromising the microgrid data integrity and availability, namely FDI and DoS/DDoS cyber-attacks. Mathematical models for the attacks are developed and performance indices are rigorously defined to provide a mean for cyber-attack physical impact quantification. The impact assessment results are then used to facilitate the proposition of novel mitigation strategies, to test their performance and evaluate their effectiveness in enhancing the resiliency and robustness of the microgrid control infrastructure to resist cyber intrusions. Enhanced supplementary control loops added at the primary and secondary control levels are proposed to provide attack compensation and post-attack recovery in the event of FDI cyber-attacks. A novel rule-based fallback control strategy is proposed to mitigate DoS/DDoS cyber-attacks and provide coordination amongst DERs in a partially or fully-decentralized manner. A multi-stage cyber resilient control infrastructure is then developed to embed cyber security into the microgrid's design to ensure resiliency, robustness and reliability in the event of cyber-attacks. A real-time HIL co-simulation platform modeling and interfacing the microgrid power system, information and communication network layers is presented and used to analyze the impact of cyber-attacks and to test and validate the effectiveness of the proposed cyber resilient mitigation strategies. Recommendations and best cyber security practices concluded from this work are also presented. " --

Network Security Strategies Kenneth Geers

Cyber security has become a topic of concern over the past decade as private industry, public administration, commerce, and communication have gained a greater online presence. As many individual and organizational activities continue to evolve in the digital sphere, new vulnerabilities arise. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications contains a compendium of the latest academic material on new methodologies and applications in the areas of digital security and threats. Including innovative studies on cloud security, online threat protection, and cryptography, this multi-volume book is an ideal source for IT specialists, administrators, researchers, and students interested in uncovering new ways to thwart cyber breaches and protect sensitive digital information.

Protect your network and enterprise against advanced cybersecurity attacks and threats John Wiley & Sons

Every organization faces cyberthreats, cyberattacks, and technology breaches. Schools are no different. But professors, instructors, educators, and school systems have mostly failed to promote cybersecurity, leaving themselves—and their students—at risk. Joseph O. Esin highlights the serious nature of the problem in this book. He answers questions such as: • What does a well-structured plan to prevent cyber-threats look like? • How can we promote equity of cybersecurity in education system? • Where do cyber threats rank compared with other dangers? • How can high schools, colleges, and universities promote cybersecurity endeavors? The best way to prevent cyberattacks is to create a professional education alliance that promotes meaningful change. High school, colleges, universities, professors, educators, and support personnel must come to the table to make prevention a priority. Get a clear understanding of the problem and respond with meaningful measures with the insights and information in The Equity of Cybersecurity in the Education System.

Risks and Mitigation Packt Publishing Ltd

The new emphasis on physical security resulting from the terrorist threat has forced many information security professionals to struggle to maintain their organization's focus on protecting information assets. In order to command attention, they need to emphasize the broader role of information security in the strategy of their companies. Until now, however, most books about strategy and planning have focused on the production side of the business, rather than operations. Strategic Information Security integrates the importance of sound security policy with the strategic goals of an organization. It provides IT professionals and management with insight into the issues surrounding the goals of protecting valuable information assets. This text reiterates that an effective information security program relies on more than policies or hardware and software, instead it hinges on having a mindset that security is a core part of the business and not just an afterthought. Armed with the content contained in this book, security specialists can redirect the discussion of security towards the terms and concepts that management understands. This increases the likelihood of obtaining the funding and managerial support that is needed to build and maintain airtight security programs.

Department of Homeland Security Appropriations for 2012 Springer

What are the cyber vulnerabilities in supply chain management? How can firms manage cyber risk and cyber security challenges in procurement, manufacturing, and logistics?Today it is clear that supply chain is often the core area of a firm's cyber security vulnerability, and its first line of defense. This book brings together several experts from both industry and academia to shine light on this problem, and advocate solutions for firms operating in this new technological landscape.Specific topics addressed in this book include: defining the world of cyber space, understanding the connection between supply chain

management and cyber security, the implications of cyber security and supply chain risk management, the 'human factor' in supply chain cyber security, the executive view of cyber security, cyber security considerations in procurement, logistics, and manufacturing among other areas.

Hacking Techniques Used to Interfere the U.S. Election and to Exploit Government & Private Sectors, Recommended Mitigation Strategies and International Cyber-Conflict Law Routledge

Cyber-Security Threats, Actors, and Dynamic Mitigation provides both a technical and state-of-the-art perspective as well as a systematic overview of the recent advances in different facets of cyber-security. It covers the methodologies for modeling attack strategies used by threat actors targeting devices, systems, and networks such as smart homes, critical infrastructures, and industrial IoT. With a comprehensive review of the threat landscape, the book explores both common and sophisticated threats to systems and networks. Tools and methodologies are presented for precise modeling of attack strategies, which can be used both proactively in risk management and reactively in intrusion prevention and response systems. Several contemporary techniques are offered ranging from reconnaissance and penetration testing to malware detection, analysis, and mitigation. Advanced machine learning-based approaches are also included in the area of anomaly-based detection, that are capable of detecting attacks relying on zero-day vulnerabilities and exploits. Academics, researchers, and professionals in cyber-security who want an in-depth look at the contemporary aspects of the field will find this book of interest. Those wanting a unique reference for various cyber-security threats and how they are detected, analyzed, and mitigated will reach for this book often.

Cyber-Security Threats, Actors, and Dynamic Mitigation John Wiley & Sons

After scrutinizing numerous cybersecurity strategies, Microsoft’s former Global Chief Security Advisor provides unique insights on the evolution of the threat landscape and how enterprises can address modern cybersecurity challenges. Key Features Protect your organization from cybersecurity threats with field-tested strategies by the former most senior security advisor at Microsoft Discover the most common ways enterprises initially get compromised Measure the effectiveness of your organization’s current cybersecurity program against cyber attacks Book Description Cybersecurity Threats, Malware Trends, and Strategies shares numerous insights about the threats that both public and private sector organizations face and the cybersecurity strategies that can mitigate them. The book provides an unprecedented long-term view of the global threat landscape by examining the twenty-year trend in vulnerability disclosures and exploitation, nearly a decade of regional differences in malware infections, the socio-economic factors that underpin them, and how global malware has evolved. This will give you further perspectives into malware protection for your organization. It also examines internet-based threats that CISOs should be aware of. The book will provide you with an evaluation of the various cybersecurity strategies that have ultimately failed over the past twenty years, along with one or two that have actually worked. It will help executives and security and compliance professionals understand how cloud computing is a game changer for them. By the end of this book, you will know how to measure the effectiveness of your organization’s cybersecurity strategy and the efficacy of the vendors you employ to help you protect your organization and yourself. What you will learn Discover cybersecurity strategies and the ingredients critical to their success Improve vulnerability management by reducing risks and costs for your organization Learn how malware and other threats have evolved over the past decade Mitigate internet-based threats, phishing attacks, and malware distribution sites Weigh the pros and cons of popular cybersecurity strategies of the past two decades Implement and then measure the outcome of a cybersecurity strategy Learn how the cloud provides better security capabilities than on-premises IT environments Who this book is for This book is for senior management at commercial sector and public sector organizations, including Chief Information Security Officers (CISOs) and other senior managers of cybersecurity groups, Chief Information Officers (CIOs), Chief Technology Officers (CTOs) and senior IT managers who want to explore the entire spectrum of cybersecurity, from threat hunting and security risk management to malware analysis. Governance, risk, and compliance professionals will also benefit. Cybersecurity experts that pride themselves on their knowledge of the threat landscape will come to use this book as a reference.

Issues Surrounding the Cyber Security of the Electricity Infraestructure and Associated Mitigation Strategies CRC Press

EU National Cyber Security Strategy and Programs Handbook - Strategic Information and Developments

Cyber Security Enhancement Against Cyber-attacks on Microgrid Controllers AuthorHouse

Cyber attacks are a real threat to our country. This report presents the opposed views of USA and Russia on cyber security and gives insight into the activities of the Russian civilian and military intelligence Services (RIS) conducted during the 2016 U.S. presidential election campaign. The Grizzly Steppe Report provides details regarding the tools and hacking techniques used by the Russian hackers in order to interfere the 2016 U.S. elections. This activity by RIS is just part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information. In foreign countries, RIS actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases, RIS actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. This report provides technical indicators related to many of these operations, recommended mitigations, suggested actions to take in response to the indicators provided, and information on how to report such incidents to the U.S. Government. The edition also provides crucial information on the legality of hostile cyber activity at state level. While the United States and its allies are in general agreement on the legal status of conflict in cyberspace, China, Russia, and a number of like-minded nations have an entirely different concept of the applicability of international law to cyberspace.

Emerging Attacks and Mitigation Strategies Apress

"Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity is a practical leadership handbook defining a new strategy for improving cybersecurity and mitigating cyber risk. Written by two leading experts with extensive professional experience in cybersecurity, the book provides CEOs and cyber newcomers alike with novel, concrete guidance on how to implement a cutting-edge strategy to mitigate an organization's overall risk to malicious cyberattacks. Using short, real-world case studies, the book highlights the need to address attack prevention and the resilience of each digital asset while also accounting for an incident's potential impact on overall operations. In a world of hackers, artificial intelligence, and

persistent ransomware attacks, the Embedded Endurance strategy embraces the reality of interdependent digital assets and provides an approach that addresses cyber risk at both the micro- (people, networks, systems and data) and macro- (organizational) levels. Most books about cybersecurity focus entirely on technology; the Embedded Endurance strategy recognizes the need for sophisticated thinking with preventative and resilience measures engaged systematically a cross your organization"--

Understanding Cybersecurity Management in FinTech Oxford University Press

Strategic Cyber Security: Evaluating Nation-state Cyber Attack Mitigation Strategies with DEMATELCyber Security and Threats: Concepts, Methodologies, Tools, and ApplicationsConcepts, Methodologies, Tools, and ApplicationsIGI Global

Challenges, Strategies, and Trends IGI Global

Security problems have evolved in the corporate world because of technological changes, such as using the Internet as a means of communication. With this, the creation, transmission, and storage of information may represent security problem. Metrics and Methods for Security Risk Management is of interest, especially since the 9/11 terror attacks, because it addresses the ways to manage risk security in the corporate world. The book aims to provide information about the fundamentals of security risks and the corresponding components, an analytical approach to risk assessments and mitigation, and quantitative methods to assess the risk components. In addition, it also discusses the physical models, principles, and quantitative methods needed to assess the risk components. The by-products of the methodology used include security standards, audits, risk metrics, and program frameworks. Security professionals, as well as scientists and engineers who are working on technical issues related to security problems will find this book relevant and useful. Offers an integrated approach to assessing security risk Addresses homeland security as well as IT and physical security issues Describes vital safeguards for ensuring true business continuity

High Schools, Undergraduate, Graduate and Post-Graduate Studies. Cengage Learning

Enterprise Cybersecurity empowers organizations of all sizes to defend themselves with next-generation cybersecurity programs against the escalating threat of modern targeted cyberattacks. This book presents a comprehensive framework for managing all aspects of an enterprise cybersecurity program. It enables an enterprise to architect, design, implement, and operate a coherent cybersecurity program that is seamlessly coordinated with policy, programmatics, IT life cycle, and assessment. Fail-safe cyberdefense is a pipe dream. Given sufficient time, an intelligent attacker can eventually defeat defensive measures protecting an enterprise’s computer systems and IT networks. To prevail, an enterprise cybersecurity program must manage risk by detecting attacks early enough and delaying them long enough that the defenders have time to respond effectively. Enterprise Cybersecurity shows players at all levels of responsibility how to unify their organization’s people, budgets, technologies, and processes into a cost-efficient cybersecurity program capable of countering advanced cyberattacks and containing damage in the event of a breach. The authors of Enterprise Cybersecurity explain at both strategic and tactical levels how to accomplish the mission of leading, designing, deploying, operating, managing, and supporting cybersecurity capabilities in an enterprise environment. The authors are recognized experts and thought leaders in this rapidly evolving field, drawing on decades of collective experience in cybersecurity and IT. In capacities ranging from executive strategist to systems architect to cybercombatant, Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, and Abdul Aslam have fought on the front lines of cybersecurity against advanced persistent threats to government, military, and business entities.

Cybersecurity Threats with New Perspectives Routledge

Build a resilient network and prevent advanced cyber attacks and breaches Key Features Explore modern cybersecurity techniques to protect your networks from ever-evolving cyber threats Prevent cyber attacks by using robust cybersecurity strategies Unlock the secrets of network security Book Description With advanced cyber attacks severely impacting industry giants and the constantly evolving threat landscape, organizations are adopting complex systems to maintain robust and secure environments. Network Security Strategies will help you get well-versed with the tools and techniques required to protect any network environment against modern cyber threats. You'll understand how to identify security vulnerabilities across the network and how to effectively use a variety of network security techniques and platforms. Next, the book will show you how to design a robust network that provides top-notch security to protect against traditional and new evolving attacks. With the help of detailed solutions and explanations, you'll be able to monitor networks skillfully and identify potential risks. Finally, the book will cover topics relating to thought leadership and the management aspects of network security. By the end of this network security book, you'll be well-versed in defending your network from threats and be able to consistently maintain operational efficiency, security, and privacy in your environment. What you will learn Understand network security essentials, including concepts, mechanisms, and solutions to implement secure networks Get to grips with setting up and threat monitoring cloud and wireless networks Defend your network against emerging cyber threats in 2020 Discover tools, frameworks, and best practices for network penetration testing Understand digital forensics to enhance your network security skills Adopt a proactive approach to stay ahead in network security Who this book is for This book is for anyone looking to explore information security, privacy, malware, and cyber threats. Security experts who want to enhance their skill set will also find this book useful. A prior understanding of cyber threats and information security will help you understand the key concepts covered in the book more effectively.

Human Dimensions of Cybersecurity CRC Press

Focuses on learning vulnerabilities and cyber security. The book gives detail on the new threats and mitigation methods in the cyber security domain, and provides information on the new threats in new technologies such as vulnerabilities in deep learning, data privacy problems with GDPR, and new solutions.

Hearings Before a Subcommittee of the Committee on Appropriations, House of Representatives, One Hundred Twelfth Congress, First Session IGI Global

Risk detection and cyber security play a vital role in the use and success of contemporary computing. By utilizing the latest technological advances, more effective prevention techniques can be developed to protect against cyber threats. Detecting and Mitigating Robotic Cyber Security Risks is an essential reference publication for the latest research on new methodologies and applications in the areas of robotic and digital security. Featuring extensive coverage on a broad range of topics, such as authentication techniques, cloud security, and mobile robotics, this book is ideally designed for students, researchers, scientists, and engineers seeking current research on methods, models, and implementations of optimized security in digital contexts.

Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks CRC Press

This book constitutes the refereed proceedings of the

International Conference on Applications and Techniques in Information Security, ATIS 2016, held in Cairns, Australia, October 2016. The 10 revised full papers and three short papers presented together with two invited talks were carefully reviewed and selected from 38 submissions. The papers are organized in topical sections on invited speeches; attacks on data security systems; detection of attacks on data security systems; data security; data privacy.

Cyber Security And Supply Chain Management: Risks, Challenges, And Solutions Springer Nature

Complete proceedings of the 14th European Conference on Cyber Warfare and Security Hatfield UK Published by Academic Conferences and Publishing International Limited