Vendor Management Cyber Security

GAIGE MCINTYRE

Cyber Breach Response That Actually Works Routledge
Aware that a single crisis event can devastate their business, managers must be prepared for the worst from an expansive array of threats. The Routledge Companion to Risk, Crisis and Security in Business comprises a professional and scholarly collection of work in this critical field. Risks come in many varieties, and there is a growing concern for organizations to respond to the challenge. Businesses can be severely impacted by natural and man-made disasters including: floods, earthquakes, tsunami, environmental threats, terrorism, supply chain risks, pandemics, and white-collar crime. An organization’s resilience is dependent not only on their own system security and infrastructure, but also on the wider infrastructure providing health and safety, utilities, transportation, and communication. Developments in risk security and management knowledge offer a path towards resilience and recovery through effective leadership in crisis situations. The growing body of knowledge in research and methodologies is a basis for decisions to safeguard people and assets, and to ensure the survivability of an organization from a crisis. Not only can businesses become more secure through risk management, but an effective program can also facilitate innovation and afford new opportunities. With chapters written by an international selection of leading experts, this book fills a crucial gap in our current knowledge of risk, crisis and security in business by exploring a broad spectrum of topics in the field. Edited by a globally-recognized expert on risk, this book is a vital reference for researchers, professionals and students with an interest in current scholarship in this expanding discipline.
Cyber Guardians Blue Rose Publishers
Cybellium Ltd is dedicated to empowering individuals and organizations with the knowledge and skills they need to navigate the ever-evolving computer science landscape securely and learn only the latest information available on any subject in the category of computer science including: - Information Technology (IT) - Cyber Security - Information Security - Big Data - Artificial Intelligence (AI) - Engineering - Robotics - Standards and compliance Our mission is to be at the forefront of computer science education, offering a wide and comprehensive range of resources, including books, courses, classes and training

programs, tailored to meet the diverse needs of any subject in computer science. Visit https://www.cybellium.com for more books.

Cybersecurity John Wiley & Sons

A comprehensive guide to administering and protecting the latest Windows 11 and Windows server operating system from ongoing cyber threats using zero-trust security principles Key Features • Learn to protect your Windows environment using zero-trust and a multi-layered security approach • Implement security controls using Intune, Configuration Manager, Defender for Endpoint, and more • Understand how to onboard modern cyber-threat defense solutions for Windows clients Book Description Are you looking for the most current and effective ways to protect Windows-based systems from being compromised by intruders? This updated second edition is a detailed guide that helps you gain the expertise to implement efficient security measures and create robust defense solutions using modern technologies. The first part of the book covers security fundamentals with details around building and implementing baseline controls. As you advance, you'll learn how to effectively secure and harden your Windows-based systems through hardware, virtualization, networking, and identity and access management (IAM). The second section will cover administering security controls for Windows clients and servers with remote policy management using Intune, Configuration Manager, Group Policy, Defender for Endpoint, and other Microsoft 365 and Azure cloud security technologies. In the last section, you'll discover how to protect, detect, and respond with security monitoring, reporting, operations, testing, and auditing. By the end of this book, you'll have developed an understanding of the processes and tools involved in enforcing security controls and implementing zero-trust security principles to protect Windows systems. What you will learn • Build a multi-layered security approach using zero-trust concepts • Explore best practices to implement security baselines successfully • Get to grips with virtualization and networking to harden your devices • Discover the importance of identity and access management • Explore Windows device administration and remote management • Become an expert in hardening your Windows infrastructure • Audit, assess, and test to ensure controls are successfully applied and enforced • Monitor and report activities to stay on top of vulnerabilities Who this book is for If you're a cybersecurity or technology professional, solutions architect, systems engineer, systems administrator, or anyone interested in learning how to secure the latest Windows-based systems, this book is for you. A basic understanding of Windows security concepts, Intune, Configuration Manager, Windows PowerShell, and Microsoft Azure will help you get the best out of this book.

Security Risk Management Routledge

The Smart Grid has the potential to revolutionize electricity delivery systems, and the security of its infrastructure is a vital concern not only for cyber-security practitioners, engineers, policy makers, and utility executives, but also for the media and consumers. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid explores the important techniques, challenges, and forces that will shape how we achieve a secure twenty-first century electric grid. Includes a Foreword by Michael Assante, President and CEO, National Board of Information Security Examiners Following an overview of the components of the Smart Grid, the book delves into the evolution of security standards and regulations and examines ways in which the Smart Grid might be regulated. The authors discuss the technical details about how metering technology is being implemented and the likely threats and vulnerabilities that utilities will face. They address the home area network (HAN) and examine distribution and transmission—the foundation for the delivery of electricity, along with distributed generation, micro-grids, and operations. The book explores future concepts—such as energy storage and the use of plug-in electric vehicles (PEVs)—in addition to the concomitant risk for fraud and manipulation with stored energy. Consumer-related issues are discussed as they pertain to emerging ways of receiving and generating energy. The book examines dysfunctions ranging from inadvertent outages to cyber-attack and presents recommendations on how to respond to these incidents. It concludes with speculation of future cyber-security challenges and discusses new ways that the grid can be defended, such as better key management and protection. Written in a style rigorous enough for the practitioner yet accessible to a broad audience, this comprehensive volume covers a topic that is becoming more critical to industry and consumers everywhere.

What Cfo's Need to Know about Supply Chain Transactions John Wiley & Sons

Security Risk Management is the definitive guide for building or running an information security risk management program. This book teaches practical techniques that will be used on a daily basis, while also explaining the fundamentals so students understand the rationale behind these practices. It explains how to perform risk assessments for new IT projects, how to efficiently manage daily risk activities, and how to qualify the current risk level for presentation to executive level management. While other books focus entirely on risk analysis methods, this is the first comprehensive text for managing security risks. This book will help you to break free from the so-called best practices argument by articulating risk exposures in business terms. It includes case studies to provide hands-on experience using risk assessment tools to calculate the costs and benefits of any security investment. It explores each phase of the risk management lifecycle, focusing on policies and assessment processes that should be used to properly assess and mitigate risk. It also presents a roadmap for designing and implementing a security risk management program. This book will be a valuable resource for CISOs, security managers, IT managers, security consultants, IT auditors, security analysts, and students enrolled in information security/assurance college programs. Named a 2011 Best Governance and ISMS Book by InfoSec Reviews Includes case studies to provide hands-on experience using risk assessment tools to calculate the costs and benefits of any security investment Explores each phase of the risk management lifecycle, focusing on policies and assessment processes that should be used to properly assess and mitigate risk Presents a roadmap for designing and implementing a security risk management program

Stop the Cyber Bleeding CRC Press

Assessing vendors is a tricky process. Large and regulated organizations are forced to demonstrate due diligence in vendor assessment, but often do not know how to do this. This results in a great deal of busywork being required by both the vendors and the organizations. Smaller organizations don't know what to look for and, as a result, often wind up selecting based on price instead of value. This results in service failures and vendors that just milk their customers for as long as they can. Assessing Vendors shows you how to walk the line between under- and over-assessing, so decisions can be made on sufficient data without wasting time, digging too deeply, or making decisions too quickly. This hands-on guide will show you how to use an iterative approach to vendor analysis, so you can rapidly filter out the vendors that are clear failures and then select likely winners. It will then show you how to do progressively deeper dives into the likely winners so you can select a preferred vendor. Finally, you will learn how to negotiate with your preferred vendor to get

reasonable prices and services. Provides an iterative approach to vendor assessment, showing you how to make decisions on sufficient data without wasting time Includes checklists to help you navigate the decision-making process, while considering all the important factors needed to make a sound decision Helps you understand and evaluate vendors based on key concepts such as performance criteria, functional testing, production, and price Provides an iterative approach to vendor assessment, showing you how to make decisions on sufficient data without wasting time Includes checklists to help you navigate the decision-making process, while considering all the important factors needed to make a sound decision Helps you understand and evaluate vendors based on key concepts such as performance criteria, functional testing, production, and price

Cybersecurity for Executives in the Age of Cloud Packt Publishing Ltd

This SpringerBrief introduces methodologies and tools for quantitative understanding and assessment of supply chain risk to critical infrastructure systems. It unites system reliability analysis, optimization theory, detection theory and mechanism design theory to study vendor involvement in overall system security. It also provides decision support for risk mitigation. This SpringerBrief introduces I-SCRAM, a software tool to assess the risk. It enables critical infrastructure operators to make risk-informed decisions relating to the supply chain, while deploying their IT/OT and IoT systems. The authors present examples and case studies on supply chain risk assessment/mitigation of modern connected infrastructure systems such as autonomous vehicles, industrial control systems, autonomous truck platooning and more. It also discusses how vendors of different system components are involved in the overall security posture of the system and how the risk can be mitigated through vendor selection and diversification. The specific topics in this book include: Risk modeling and analysis of IoT supply chains Methodologies for risk mitigation, policy management, accountability, and cyber insurance Tutorial on a software tool for supply chain risk management of IoT These topics are supported by up-to-date summaries of the authors' recent research findings. The authors introduce a taxonomy of supply chain security and discusses the future challenges and directions in securing the supply chains of IoT systems. It also focuses on the need for joint policy and technical solutions to counter the emerging risks, where technology should inform policy and policy should regulate technology development. This SpringerBrief has self-contained chapters, facilitating the readers to peruse individual topics of interest. It provides a broad understanding of the emerging field of cyber supply chain security in the context of IoT systems to academics, industry professionals and government officials.

Mastering Windows Security and Hardening Packt Publishing Ltd

This timely Research Handbook explores the handling of city and municipal finances in the 21st century. It examines the impact of the Great Recession and COVID-19 pandemic on cities and municipalities, highlighting strengths, weaknesses, and avenues for future progress in city and municipal financial management.

Why CISOs Fail Edward Elgar Publishing

"This is the book executives have been waiting for. It is clear: With deep expertise but in nontechnical language, it describes what cybersecurity risks are and the decisions executives need to make to address them. It is crisp: Quick and to the point, it doesn't waste words and won't waste your time. It is candid: There is no sure cybersecurity defense, and Chris Moschovitis doesn't pretend there is; instead, he tells you how to understand your company's risk and make smart business decisions about what you can mitigate and what you cannot. It is also, in all likelihood, the only book ever written (or ever to be written) about cybersecurity defense that is fun to read." —Thomas A. Stewart, Executive Director, National Center for the Middle Market and Co-Author of Woo, Wow, and Win: Service Design, Strategy, and the Art of Customer Delight Get answers to all your cybersecurity questions In 2016, we reached a tipping point—a moment where the global and local implications of cybersecurity became undeniable. Despite the seriousness of the topic, the term "cybersecurity" still exasperates many people. They feel terrorized and overwhelmed. The majority of business people have very little understanding of cybersecurity, how to manage it, and what's really at risk. This essential guide, with its dozens of examples and case studies, breaks down every element of the development and management of a cybersecurity program for the executive. From understanding the need, to core risk management principles, to threats, tools, roles and responsibilities, this book walks the reader through each step of developing and implementing a cybersecurity program. Read cover-to-cover, it's a thorough overview, but it can also function as a useful reference book as individual questions and difficulties arise. Unlike other cybersecurity books, the text is not bogged down with industry jargon Speaks specifically to the executive who is not familiar with the development or implementation of cybersecurity programs Shows you how to make pragmatic, rational, and informed decisions for your organization Written by a top-flight technologist with decades of experience and a track record of success If you're a business manager or executive who needs to make sense of cybersecurity, this book demystifies it for you.

The Routledge Companion to Risk, Crisis and Security in Business Routledge

IT and cybersecurity teams have had a long-standing battle between functionality and security. But why? To understand where the problem lies, this book will explore the different job functions, goals, relationships, and other factors that may impact how IT and cybersecurity teams interact. With different levels of budget, competing goals, and a history of lack of communication, there is a lot of work to do to bring these teams together. Empathy and emotional intelligence are common phenomena discussed in leadership books, so why not at the practitioner level? Technical teams are constantly juggling projects, engineering tasks, risk management activities, security configurations, remediating audit findings, and the list goes on. Understanding how psychology and human factors engineering practices can improve both IT and cybersecurity teams can positively impact those relationships, as well as strengthen both functionality and security. There is no reason to have these teams at odds or competing for their own team's mission; align the missions, and align the teams. The goal is to identify the problems in your own team or organization and apply the principles within to improve how teams communicate, collaborate, and compromise. Each organization will have its own unique challenges but following the question guide will help to identify other technical gaps horizontally or vertically.

Optimal Spending on Cybersecurity Measures John Wiley & Sons

Many CFOs know little about the thousands of daily supply chain transactions that affect their companies. These transactions are often viewed as "routine" and are largely ignored by senior management, despite the fact that they pose huge potential risks to the organization. The sheer number of the daily supply chain transactions makes mistakes and missed opportunities a huge risk. Moreover, these transactions expose the company to potential claims and lawsuits. Poorly defined responsibilities inevitably lead to busted budgets and failed objectives. CFOs owe it to their company and their careers to be knowledgeable about supply chain transactions. This book addresses those issues and

has been acclaimed by CFOs and academics alike. Here is what others have said about the book: "By applying the knowledge found in this book, CFOs and COOs can better navigate through unchartered waters and, when appropriate, constructively challenge the business decisions being made. This book is a great resource for all existing or aspiring CFOs or COOs, who want to improve their capabilities regarding contracts and contract management in order to avoid, manage, or mitigate financial risks." Rahul Agarwal, CFA is the Chief Financial Officer for CIFC Corporation, New York City. "Paul Humbert's latest book is a comprehensive resource for executives and managers involved with creating, executing, or managing transactions locally and globally. Each chapter provides actionable insights and tools to manage one's transactions throughout an organization from "cradle to grave" in an easy to digest format." David Dreyfus, Associate Professor, Department of Supply Chain Management Rutgers Business School - Newark and New Brunswick, New Jersey. "In the section of identifying and evaluating risks, I found the topic of cyber-security of particular interest as vendor management has been a key focus of regulators." James Ruggerio, Jr., CFA, CPA, Chief Operating Officer for Chatham Asset Management, LLC. "The book is very well written . . . which makes it eminently accessible to the public and especially useful to supply chain managers and CFOs." Benjamin Melamed, Distinguished Professor, Department of Supply Chain Management Rutgers Business School - Newark and New Brunswick, New Jersey. Commercially unwise behaviors both before and after the contract is signed or purchase order issue, results in loss of rights and remedies as well as claims and lawsuits. This book empowers CFOs to ask the right questions to ensure that inherent commercial risks are properly addressed.

Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal City of London College of Economics

A comprehensive overview for directors aiming to meet their cybersecurity responsibilities In Cyber Guardians: Empowering Board Members for Effective Cybersecurity, veteran cybersecurity advisor Bart McDonough delivers a comprehensive and hands-on roadmap to effective cybersecurity oversight for directors and board members at organizations of all sizes. The author includes real-world case studies, examples, frameworks, and blueprints that address relevant cybersecurity risks, including the industrialized ransomware attacks so commonly found in today’s headlines. In the book, you’ll explore the modern cybersecurity landscape, legal and regulatory requirements, risk management and assessment techniques, and the specific role played by board members in developing and promoting a culture of cybersecurity. You’ll also find: Examples of cases in which board members failed to adhere to regulatory and legal requirements to notify the victims of data breaches about a cybersecurity incident and the consequences they faced as a result Specific and actional cybersecurity implementation strategies written for readers without a technical background What to do to prevent a cybersecurity incident, as well as how to respond should one occur in your organization A practical and accessible resource for board members at firms of all shapes and sizes, Cyber Guardians is relevant across industries and sectors and a must-read guide for anyone with a stake in robust organizational cybersecurity.

Managing Cyber Risk CRC Press

Cyber risk is the highest perceived business risk according to risk managers and corporate insurance experts. Cybersecurity typically is viewed as the boogeyman: it strikes fear into the hearts of non-technical employees. Enterprise Cybersecurity in Digital Business: Building a Cyber Resilient Organization provides a clear guide for companies to understand cyber from a business perspective rather than a technical perspective, and to build resilience for their business. Written by a world-renowned expert in the field, the book is based on three years of research with the Fortune 1000 and cyber insurance industry carriers, reinsurers, and brokers. It acts as a roadmap to understand cybersecurity maturity, set goals to increase resiliency, create new roles to fill business gaps related to cybersecurity, and make cyber inclusive for everyone in the business. It is unique since it provides strategies and learnings that have shown to lower risk and demystify cyber for each person. With a clear structure covering the key areas of the Evolution of Cybersecurity, Cybersecurity Basics, Cybersecurity Tools, Cybersecurity Regulation, Cybersecurity Incident Response, Forensics and Audit, GDPR, Cybersecurity Insurance, Cybersecurity Risk Management, Cybersecurity Risk Management Strategy, and Vendor Risk Management Strategy, the book provides a guide for professionals as well as a key text for students studying this field. The book is essential reading for CEOs, Chief Information Security Officers, Data Protection Officers, Compliance Managers, and other cyber stakeholders, who are looking to get up to speed with the issues surrounding cybersecurity and how they can respond. It is also a strong textbook for postgraduate and executive education students in cybersecurity as it relates to business.

Financial Cybersecurity Risk Management CRC Press

An introductory guide to managing cybersecurity for businesses. How to prevent, protect and respond to threats. Providing an insight to the extent and scale a potential damage could cause when there is a breech in cyber security. It includes case studies and advice from leading industry professionals, giving you the necessary strategies and resources to prevent, protect and respond to any threat:• Introduction to cyber security• Security framework• Support services for UK public and private sectors• Cyber security developments• Routing a map for resilience• Protecting financial data• Countermeasures to advance threats• Managing incidents and breaches• Preparing for further threats• Updating contingency plans

Cybersecurity Program Development for Business Legend Press

This book serves as an introduction into the world of security and provides insight into why and how current security management practices fail, resulting in overall dissatisfaction by practitioners and lack of success in the corporate environment. The author examines the reasons and suggests how to fix them. The resulting improvement is highly beneficial to any corporation that chooses to pursue this approach or strategy and from a bottom-line and business operations perspective, not just in technical operations. This book transforms the understanding of the role of the CISO, the selection process for a CISO, and the financial impact that security plays in any organization.

Managing Cybersecurity in the Process Industries WIT Press

This book gives insight into the legal aspects of data ownership in the 21st century. With the amount of information being produced and collected growing at an ever accelerating rate, governments are implementing laws to regulate the use of this information by corporations. Companies are more likely than ever to face heavy lawsuits and sanctions for any misuse of information, which includes data breaches caused by cybercriminals. This book serves as a guide to all companies that collect customer information, by giving instructions on how to avoid making these costly mistakes and to ensure they are not liable in the event of stolen information.

Information Security Handbook Routledge

Learn how to implement a comprehensive third party risk programme which complies with regulation and is aligned with business goals.

Awareness Handbook on Cyber Security framework & Digital Banking Payments Security Springer Nature
Accelerate your journey of securing safety-critical automotive systems through practical and standard-compliant methods Key Features Understand how automotive systems can become vulnerable to cyberattacks Apply security controls to all vehicle layers for mitigating cybersecurity risks Find out how systematic secure engineering mitigates cyber risks while ensuring compliance Purchase of the print or Kindle book includes a free PDF eBook Book DescriptionReplete with exciting challenges, automotive cybersecurity is an emerging domain, and cybersecurity is a foundational enabler for current and future connected vehicle features. This book addresses the severe talent shortage faced by the industry in meeting the demand for building cyber-resilient systems by consolidating practical topics on securing automotive systems to help automotive engineers gain a competitive edge. The book begins by exploring present and future automotive vehicle architectures, along with relevant threats and the skills essential to addressing them. You'll then explore cybersecurity engineering methods, focusing on compliance with existing automotive standards while making the process advantageous. The chapters are designed in a way to help you with both the theory and practice of building secure systems while considering the cost, time, and resource limitations of automotive engineering. The concluding chapters take a practical approach to threat modeling automotive systems and teach you how to implement security controls across different vehicle architecture layers. By the end of this book, you'll have learned effective methods of handling cybersecurity risks in any automotive product, from single libraries to entire vehicle architectures.What you will learn Get to grips with present and future vehicle networking technologies Explore basic concepts for securing automotive systems Discover diverse approaches to threat modeling of systems Conduct efficient threat analysis and risk assessment (TARA) for automotive systems using best practices Gain a comprehensive understanding of ISO/SAE 21434's cybersecurity engineering approach Implement cybersecurity controls for all vehicle life cycles Master ECU-level cybersecurity controls Who this book is forIf you're an engineer wondering where to get started in the field of automotive cybersecurity or trying to understand which security standards apply to your product and how, then this is the book for you. This book is also for experienced engineers looking for a practical approach to automotive cybersecurity development that can be achieved within a reasonable time frame while leveraging established safety and quality processes. Familiarity with basic automotive development processes across the V-model will help you make the most of this book.

Zero Trust and Third-Party Risk Cybellium Ltd
Dramatically lower the cyber risk posed by third-party software and vendors in your organization In Zero Trust and Third-Party Risk, veteran cybersecurity leader Gregory Rasner delivers an accessible and authoritative walkthrough of the fundamentals and finer points of the zero trust philosophy and its application to the mitigation of third-party cyber risk. In this book, you'll explore how to build a zero trust program and nurture it to maturity. You will also learn how and why zero trust is so effective in reducing third-party cybersecurity risk. The author uses the story of a fictional organization—KC Enterprises—to illustrate the real-world application of zero trust principles. He takes you through a full zero trust implementation cycle, from initial breach to cybersecurity program maintenance and upkeep. You'll also find: Explanations of the processes, controls, and programs that make up the zero trust doctrine Descriptions of the five pillars of implementing zero trust with third-party vendors Numerous examples, use-cases, and stories that highlight the real-world utility of zero trust An essential resource for board members, executives, managers, and other business leaders, Zero Trust and Third-Party Risk will also earn a place on the bookshelves of technical and cybersecurity practitioners, as well as compliance professionals seeking effective strategies to dramatically lower cyber risk.

Mastering Attack Surface Management John Wiley & Sons
Created by the AICPA, this authoritative guide provides interpretative guidance to enable accountants to examine and report on an entity's cybersecurity risk managementprogram and controls within that program. The guide delivers a framework which has been designed to provide stakeolders with useful, credible information about the effectiveness of an entity's cybersecurity efforts.

Related with Vendor Management Cyber Security:
© Vendor Management Cyber Security The Law Is Like A Mirror Bible Verse
© Vendor Management Cyber Security The Law Group Wilmington Nc
© Vendor Management Cyber Security The Language Of Science Worksheet Answers Key