

Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

This book explores a broad cross section of research and actual case studies to draw out new insights that may be used to build a benchmark for IT security professionals. This research takes a deeper dive beneath the surface of the analysis to uncover novel ways to mitigate data security vulnerabilities, connect the dots and identify patterns in the data on breaches. This analysis will assist security professionals not only in benchmarking their risk management programs but also in identifying forward looking security measures to narrow the path of future vulnerabilities.

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.

Modern web applications are built on a tangle of technologies that have been developed over time and then haphazardly pieced together. Every piece of the web application stack, from HTTP requests to browser-side scripts, comes with important yet subtle security consequences. To keep users safe, it is essential for developers to confidently navigate this landscape. In *The Tangled Web*, Michal Zalewski, one of the world's top browser security experts, offers a compelling narrative that explains exactly how browsers work and why they're fundamentally insecure. Rather than dispense simplistic advice on vulnerabilities, Zalewski examines the entire browser security model, revealing weak points and providing crucial information for shoring up web application security. You'll learn how to: –Perform common but surprisingly complex tasks such as URL parsing and HTML sanitization –Use modern security features like Strict Transport Security, Content Security Policy, and Cross-Origin Resource Sharing –Leverage many variants of the same-origin policy to safely compartmentalize complex web applications and protect user credentials in case of XSS bugs –Build mashups and embed gadgets without getting stung by the tricky frame navigation policy –Embed or host user-supplied content without running into the trap of content sniffing For quick reference, "Security Engineering Cheat Sheets" at the end of each chapter offer ready solutions to problems you're most likely to encounter. With coverage extending as far as planned HTML5 features, *The Tangled Web* will help you create secure web applications that stand the test of time.

Learn how to perform project management according to international standards of compliance using capability assessment processes. This book compares and contrasts the approach to project management using ISO 21500 against the more direct ISO 33000 Capability Assessment. It shows how to assess projects adequately for process improvement or how well an organization performs against a standard, measurable framework. Using ISO 21500 as the project management reference point and ISO 15504/33000 as the capability assessment reference, the book shows you how to assess whether your projects are being run according to a specific capability level or support them to reach higher levels of capability.

Internal auditors must know many concepts, techniques, control frameworks, and remain knowledgeable despite the many changes occurring

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

in the marketplace and their profession. This easy to use reference makes this process easier and ensures auditors can obtain needed information quickly and accurately. This book consists of 100 topics, concepts, tips, tools and techniques that relate to how internal auditors interact with internal constituencies and addresses a variety of technical and non-technical subjects. Non-auditors have an easy-to-use guide that increases their understanding of what internal auditors do and how, making it easier for them to partner with them more effectively.

This book discusses various common occupational and organizational fraud schemes, based on the Association of Certified Fraud Examiners (ACFE) fraud tree and assist fraud examiners and auditors in correctly choosing the appropriate audit tests to uncover such various fraud schemes. The book also includes information about audit test red flags to watch out for, a list of recommended controls to help prevent future fraud related incidents, as well as step-by-step demonstrations of a number of common audit tests using IDEA® as a CAATT tool.

Operational Assessment of IT presents ideas and concepts of optimization designed to improve an organization's business processes and assist business units in meeting organizational goals more effectively. Rather than focus on specific technologies, computing environments, enterprise risks, resource programs, or infrastructure, the book focuses on

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.

"Drawing upon a wealth of experience from academia, industry, and government service, this book details and dissects current organizational cybersecurity policy issues on a global scale. Using simple language, it includes a thorough description of each issue, lists pros and cons, documents policy alternatives for the sake of clarity with respect to policy alone, and dives into organizational implementation issues. It also equips the reader with descriptions of the impact of specific policy choices, both positive and negative. This book gives students, scholars, and technical decision-makers the necessary knowledge of cybersecurity policy in order to make more informed decisions"--Provided by publisher.

This book presents a standard methodology approach to cyber-resilience. Readers will learn how to design a cyber-resilient architecture for a given organization as well as how to maintain a state of cyber-resilience in its day-to-day operation. Readers will know how to establish a state of systematic cyber-resilience within this structure and how to evolve the protection to correctly address the threat environment. This revolves around the steps to perform strategic cyber-resilience planning, implementation and evolution. Readers will know how to perform the necessary activities to identify, prioritize and deploy targeted controls and maintain a persistent and reliable reporting system.

Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE) introduces a new methodology to help critical infrastructure owners, operators and their security practitioners make demonstrable improvements in securing their most important functions and processes. Current best practice approaches to cyber defense struggle to stop targeted attackers from creating potentially catastrophic results. From a national security perspective, it is not just the damage to the military, the economy, or essential critical infrastructure companies that is a concern. It is the cumulative, downstream effects from potential regional blackouts, military mission kills, transportation stoppages, water delivery or treatment issues, and so on. CCE is a validation that engineering first principles can be applied to

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

the most important cybersecurity challenges and in so doing, protect organizations in ways current approaches do not. The most pressing threat is cyber-enabled sabotage, and CCE begins with the assumption that well-resourced, adaptive adversaries are already in and have been for some time, undetected and perhaps undetectable. Chapter 1 recaps the current and near-future states of digital technologies in critical infrastructure and the implications of our near-total dependence on them. Chapters 2 and 3 describe the origins of the methodology and set the stage for the more in-depth examination that follows. Chapter 4 describes how to prepare for an engagement, and chapters 5-8 address each of the four phases. The CCE phase chapters take the reader on a more granular walkthrough of the methodology with examples from the field, phase objectives, and the steps to take in each phase. Concluding chapter 9 covers training options and looks towards a future where these concepts are scaled more broadly.

The Audit Value Factor: Making Management's Head Turn empowers readers with a systematic method to build and maintain a value-centric internal audit organization. The book explores how to identify, quantify, and articulate value for customers. It details six critical success factors: Value propositions that link directly to customer needs Fostering customer relationships using the CREATE model Talent development using the TEAM model Risk expertise that raises awareness, understanding, and action Change management and process optimization using the SMART model Data analytics that provide powerful insights to operations The Audit Value Factor offers easy to use tools and practical strategies that deliver tangible and immediate benefits for the internal audit team. Praise for The Audit Value Factor: Making Management's Head Turn "Daniel Samson, the inspiring and forward-thinking CAE at SRI International, has created an essential guide to adding value through Internal Audit in his new book The Audit Value Factor. It's an important addition to any internal auditor's toolkit, with helpful suggestions on topics ranging from talent planning to data analytics. I highly recommend it to any internal audit professional looking to "up their game." Laurie A. Hanover, CIA, CAE Sunrun Inc. "Internal Auditors often strive for a 'seat at the table,' be it with Business Leaders, Senior Management, the Board, or really, any significant decision maker in an organization. In The Audit Value Factor, Dan Samson provides the roadmap to ensuring that Internal Audit gets not only that seat at the table, but also that role of a critical business partner that is valued in facilitating change and helping an organization achieve its goals." Brian Tremblay, CAE Acacia Communications "Great audit functions generate value and build leadership capacity from staff to CAE. The Audit Value Factor's compelling examples, data, and actionable tools enable auditors at every level to build relationships of trust, ask the right questions, and deliver powerful insights to their organization." Dr. Kathryn Bingham, Executive Coach and CEO, LEADistics LLC

Operational Auditing: Principles and Techniques for a Changing World, 2nd edition, explains the proven approaches and essential procedures to perform risk-based operational audits. It shows how to effectively evaluate the relevant dynamics associated with programs and processes, including operational, strategic, technological, financial and compliance objectives and risks. This book merges traditional internal audit concepts and practices with contemporary quality control methodologies, tips, tools and techniques. It explains how internal auditors can perform operational audits that result in meaningful findings and useful recommendations to help organizations meet objectives and improve the perception of internal auditors as high-value contributors, appropriate change agents and trusted advisors. The 2nd edition introduces or expands the previous coverage of: • Control self-assessments. • The 7 Es framework for operational quality. • Linkages to ISO 9000. • Flowcharting techniques and value-stream analysis • Continuous monitoring. • The use of Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs). • Robotic process automation (RPA), artificial intelligence (AI) and machine learning (ML); and • Adds a new chapter that will examine the role of organizational structure and its impact on effective communications, task allocation, coordination, and

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

operational resiliency to more effectively respond to market demands.

The author examines the linkages and similarities between compulsive athletics and eating disorders, and proposes that they are different manifestations of a single condition: the activity disorder.

Welcome to the all-new second edition of Navigating the Digital Age. This edition brings together more than 50 leaders and visionaries from business, science, technology, government, academia, cybersecurity, and law enforcement. Each has contributed an exclusive chapter designed to make us think in depth about the ramifications of this digital world we are creating. Our purpose is to shed light on the vast possibilities that digital technologies present for us, with an emphasis on solving the existential challenge of cybersecurity. An important focus of the book is centered on doing business in the Digital Age—particularly around the need to foster a mutual understanding between technical and non-technical executives when it comes to the existential issues surrounding cybersecurity. This book has come together in three parts. In Part 1, we focus on the future of threat and risks. Part 2 emphasizes lessons from today's world, and Part 3 is designed to help you ensure you are covered today. Each part has its own flavor and personality, reflective of its goals and purpose. Part 1 is a bit more futuristic, Part 2 a bit more experiential, and Part 3 a bit more practical. How we work together, learn from our mistakes, deliver a secure and safe digital future—those are the elements that make up the core thinking behind this book. We cannot afford to be complacent. Whether you are a leader in business, government, or education, you should be knowledgeable, diligent, and action-oriented. It is our sincerest hope that this book provides answers, ideas, and inspiration. If we fail on the cybersecurity front, we put all of our hopes and aspirations at risk. So we start this book with a simple proposition: When it comes to cybersecurity, we must succeed.

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

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

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.

Todd Fitzgerald, co-author of the ground-breaking (ISC)2 CISO Leadership: Essential Principles for Success, Information Security Governance Simplified: From the Boardroom to the Keyboard, co-author for the E-C Council CISO Body of Knowledge, and contributor to many others including Official (ISC)2 Guide to the CISSP CBK, COBIT 5 for Information Security, and ISACA CSX Cybersecurity Fundamental Certification, is back with this new book incorporating practical experience in leading, building, and sustaining an information security/cybersecurity program. CISO COMPASS includes personal, pragmatic perspectives and lessons learned of over 75 award-winning CISOs, security leaders, professional association leaders, and cybersecurity standard setters who have fought the tough battle. Todd has also, for the first time, adapted the McKinsey 7S framework (strategy, structure, systems, shared values, staff, skills and style) for organizational effectiveness to the practice of leading cybersecurity to structure the content to ensure comprehensive coverage by the CISO and security leaders to key issues impacting the delivery of the cybersecurity strategy and demonstrate to the Board of Directors due diligence. The insights will assist the security leader to create programs appreciated and supported by the organization, capable of industry/ peer award-winning recognition, enhance cybersecurity maturity, gain confidence by senior management, and avoid pitfalls. The book is a comprehensive, soup-to-nuts book enabling security leaders to effectively protect information assets and build award-winning programs by covering topics such as developing cybersecurity strategy, emerging trends and technologies, cybersecurity organization structure and reporting models, leveraging current incidents, security control frameworks, risk management, laws and regulations, data protection and privacy, meaningful policies and procedures, multi-generational workforce team dynamics, soft skills, and communicating with the Board of Directors and executive management. The book is valuable to current and future security leaders as a valuable resource and an integral part of any college program for information/ cybersecurity.

Using the factor analysis of information risk (FAIR) methodology developed over ten years and adopted by corporations worldwide, Measuring and Managing Information Risk provides a proven and credible framework for understanding, measuring, and analyzing information risk of any size or complexity. Intended for organizations that need to either build a risk management program from the ground up or strengthen an existing one, this book provides a unique and fresh perspective on how to do a basic quantitative risk analysis. Covering such key areas as risk theory, risk calculation, scenario modeling, and communicating risk within the organization, Measuring and Managing Information Risk helps managers make better business decisions by understanding their organizational risk. Uses factor analysis of information risk (FAIR) as a methodology for measuring and managing risk in any organization. Carefully balances theory with practical applicability and relevant stories of successful implementation. Includes examples from a wide variety of businesses and situations presented in an accessible writing style.

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

A reluctant young hero must chase down an evil serpent king in “this satisfying middle-grade adventure . . . in colonial British West Africa” (Kirkus Reviews). Nate Fludd is back in the camel saddle in pursuit of a missing, deadly basilisk—the mythical King of Serpents. As if saving a Dhughani village from the beast isn’t hard enough, Nate and Aunt Phil must begin to solve the mystery of his parents’ disappearance and protect The Fludd Book of Beasts from a sinister man who always seems to be one step ahead of them. With more lively illustrations by Kelly Murphy, The Basilisk’s Lair picks up immediately where the first book in the series, Flight of the Phoenix, left off. This historical fantasy chapter book series is perfect for intermediate readers.

You may regard cloud computing as an ideal way for your company to control IT costs, but do you know how private and secure this service really is? Not many people do. With Cloud Security and Privacy, you'll learn what's at stake when you trust your data to the cloud, and what you can do to keep your virtual infrastructure and web applications secure. Ideal for IT staffers, information security and privacy practitioners, business managers, service providers, and investors alike, this book offers you sound advice from three well-known authorities in the tech security world. You'll learn detailed information on cloud computing security that-until now-has been sorely lacking. Review the current state of data security and storage in the cloud, including confidentiality, integrity, and availability Learn about the identity and access management (IAM) practice for authentication, authorization, and auditing of the users accessing cloud services Discover which security management frameworks and standards are relevant for the cloud Understand the privacy aspects you need to consider in the cloud, including how they compare with traditional computing models Learn the importance of audit and compliance functions within the cloud, and the various standards and frameworks to consider Examine security delivered as a service-a different facet of cloud security

Most organizations have been caught off-guard with the proliferation of smart devices. The IT organization was comfortable supporting the Blackberry due to its ease of implementation and maintenance. But the use of Android and iOS smart devices have created a maintenance nightmare not only for the IT organization but for the IT auditors as well. This book will serve as a guide to IT and Audit professionals on how to manage, secure and audit smart device. It provides guidance on the handling of corporate devices and the Bring Your Own Devices (BYOD) smart devices.

"I highly recommend Mr. Hobbs' book." - Stephen Thomas, PE, Founder and Editor of FunctionalSafetyEngineer.com Safety-critical devices, whether medical, automotive, or industrial, are increasingly dependent on the correct operation of sophisticated software. Many standards have appeared in the last decade on how such systems should be designed and built. Developers, who previously only had to know how to program devices for their industry, must now understand remarkably esoteric development practices and be prepared to justify their work to external auditors. Embedded Software Development for Safety-Critical Systems discusses the development of safety-critical systems under the following standards: IEC 61508; ISO 26262; EN 50128; and IEC 62304. It details the advantages and disadvantages of many architectural and design practices recommended in the standards, ranging from replication and diversification, through anomaly detection to the so-called "safety bag" systems. Reviewing the use of open-source components in safety-critical systems, this book has evolved from a course text used by QNX Software Systems for a

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

training module on building embedded software for safety-critical devices, including medical devices, railway systems, industrial systems, and driver assistance devices in cars. Although the book describes open-source tools for the most part, it also provides enough information for you to seek out commercial vendors if that's the route you decide to pursue. All of the techniques described in this book may be further explored through hundreds of learned articles. In order to provide you with a way in, the author supplies references he has found helpful as a working software developer. Most of these references are available to download for free.

The book presents the concepts of ICT supply chain risk management from the perspective of NIST IR 800-161. It covers how to create a verifiable audit-based control structure to ensure comprehensive security for acquired products. It explains how to establish systematic control over the supply chain and how to build auditable trust into the products and services acquired by the organization. It details a capability maturity development process that will install an increasingly competent process and an attendant set of activities and tasks within the technology acquisition process. It defines a complete and correct set of processes, activities, tasks and monitoring and reporting systems.

Many companies move workloads to the cloud only to encounter issues with legacy processes and organizational structures. How do you design new operating models for this environment? This practical book shows IT managers, CIOs, and CTOs how to address the hardest part of any cloud transformation: the people and the processes. Author Mike Kavis (Architecting the Cloud) explores lessons learned from enterprises in the midst of cloud transformations. You'll learn how to rethink your approach from a technology, process, and organizational standpoint to realize the promise of cost optimization, agility, and innovation that public cloud platforms provide. Learn the difference between working in a data center and operating in the cloud Explore patterns and anti-patterns for organizing cloud operating models Get best practices for making the organizational change required for a move to the cloud Understand why site reliability engineering is essential for cloud operations Improve organizational performance through value stream mapping

This book defines what IoT Systems manageability looks like and what the associated resources and costs are of that manageability. It identifies IoT Systems performance expectations and addresses the difficult challenges of determining actual costs of IoT Systems implementation, operation, and management across multiple institutional organizations. It details the unique challenges that cities and institutions have in implementing and operating IoT Systems.

This book explores the genesis of ransomware and how the parallel emergence of encryption technologies has elevated ransomware to become the most prodigious cyber threat that enterprises are confronting. It also investigates the driving forces behind what has been dubbed the 'ransomware revolution' after a series of major attacks beginning in 2013, and how the advent of cryptocurrencies provided the catalyst for the development and increased profitability of ransomware, sparking a phenomenal rise in the number and complexity of ransomware attacks. This book analyzes why the speed of technology adoption has been a fundamental factor in the continued success of financially motivated cybercrime, and how the ease of public access to advanced encryption techniques has allowed malicious actors to continue to operate with increased anonymity across the internet. This anonymity has enabled increased collaboration between attackers, which has

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

aided the development of new ransomware attacks, and led to an increasing level of technical complexity in ransomware attacks. This book highlights that the continuous expansion and early adoption of emerging technologies may be beyond the capacity of conventional risk managers and risk management frameworks. Researchers and advanced level students studying or working in computer science, business or criminology will find this book useful as a reference or secondary text. Professionals working in cybersecurity, cryptography, information technology, financial crime (and other related topics) will also welcome this book as a reference.

Software Quality Assurance: Integrating Testing, Security, and Audit focuses on the importance of software quality and security. It defines various types of testing, recognizes factors that propose value to software quality, and provides theoretical and real-world scenarios that offer value and contribute quality to projects and applications. The p

Security Smarts for the Self-Guided IT Professional “An extraordinarily thorough and sophisticated explanation of why you need to measure the effectiveness of your security program and how to do it. A must-have for any quality security program!” —Dave Cullinane, CISSP, CISO & VP, Global Fraud, Risk & Security, eBay Learn how to communicate the value of an information security program, enable investment planning and decision making, and drive necessary change to improve the security of your organization. **Security Metrics: A Beginner's Guide** explains, step by step, how to develop and implement a successful security metrics program. This practical resource covers project management, communication, analytics tools, identifying targets, defining objectives, obtaining stakeholder buy-in, metrics automation, data quality, and resourcing. You'll also get details on cloud-based security metrics and process improvement. Templates, checklists, and examples give you the hands-on help you need to get started right away. **Security Metrics: A Beginner's Guide** features: Lingo--Common security terms defined so that you're in the know on the job IMHO--Frank and relevant opinions based on the author's years of industry experience Budget Note--Tips for getting security technologies and processes into your organization's budget In Actual Practice--Exceptions to the rules of security explained in real-world contexts Your Plan--Customizable checklists you can use on the job now Into Action--Tips on how, why, and when to apply new skills and techniques at work Caroline Wong, CISSP, was formerly the Chief of Staff for the Global Information Security Team at eBay, where she built the security metrics program from the ground up. She has been a featured speaker at RSA, ITWeb Summit, Metricon, the Executive Women's Forum, ISC2, and the Information Security Forum.

All the Knowledge You Need to Build Cybersecurity Programs and Policies That Work Clearly presents best practices, governance frameworks, and key standards Includes focused coverage of healthcare, finance, and PCI DSS compliance An essential and invaluable guide for leaders, managers, and technical professionals Today, cyberattacks can place entire organizations at risk. Cybersecurity can no longer be delegated to specialists: success requires everyone to work together, from leaders on down. **Developing Cybersecurity Programs and Policies** offers start-to-finish guidance for establishing effective cybersecurity in any organization. Drawing on more than 20 years of real-world experience, Omar Santos presents realistic best practices for defining policy and governance, ensuring compliance, and collaborating to harden the entire organization. First, Santos shows how to develop workable cybersecurity policies and an effective framework for governing them. Next, he addresses risk management, asset management, and data loss prevention, showing how to align functions from HR to physical security. You'll discover best practices for securing communications, operations, and access; acquiring, developing, and maintaining technology; and responding to incidents. Santos concludes with detailed coverage of compliance in finance and healthcare, the crucial Payment Card Industry Data Security Standard (PCI DSS) standard, and the NIST Cybersecurity Framework. Whatever your current responsibilities, this guide will help you plan, manage, and lead cybersecurity—and safeguard all the assets that matter. Learn How To ·

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

Establish cybersecurity policies and governance that serve your organization's needs · Integrate cybersecurity program components into a coherent framework for action · Assess, prioritize, and manage security risk throughout the organization · Manage assets and prevent data loss · Work with HR to address human factors in cybersecurity · Harden your facilities and physical environment · Design effective policies for securing communications, operations, and access · Strengthen security throughout the information systems lifecycle · Plan for quick, effective incident response and ensure business continuity · Comply with rigorous regulations in finance and healthcare · Plan for PCI compliance to safely process payments · Explore and apply the guidance provided by the NIST Cybersecurity Framework

A fast, hands-on introduction to offensive hacking techniques Hands-On Hacking teaches readers to see through the eyes of their adversary and apply hacking techniques to better understand real-world risks to computer networks and data. Readers will benefit from the author's years of experience in the field hacking into computer networks and ultimately training others in the art of cyber-attacks. This book holds no punches and explains the tools, tactics and procedures used by ethical hackers and criminal crackers alike. We will take you on a journey through a hacker's perspective when focused on the computer infrastructure of a target company, exploring how to access the servers and data. Once the information gathering stage is complete, you'll look for flaws and their known exploits—including tools developed by real-world government financed state-actors. • An introduction to the same hacking techniques that malicious hackers will use against an organization • Written by infosec experts with proven history of publishing vulnerabilities and highlighting security flaws • Based on the tried and tested material used to train hackers all over the world in the art of breaching networks • Covers the fundamental basics of how computer networks are inherently vulnerable to attack, teaching the student how to apply hacking skills to uncover vulnerabilities We cover topics of breaching a company from the external network perimeter, hacking internal enterprise systems and web application vulnerabilities. Delving into the basics of exploitation with real-world practical examples, you won't find any hypothetical academic only attacks here. From start to finish this book will take the student through the steps necessary to breach an organization to improve its security. Written by world-renowned cybersecurity experts and educators, Hands-On Hacking teaches entry-level professionals seeking to learn ethical hacking techniques. If you are looking to understand penetration testing and ethical hacking, this book takes you from basic methods to advanced techniques in a structured learning format.

An urgent warning from two bestselling security experts--and a gripping inside look at how governments, firms, and ordinary citizens can confront and contain the tyrants, hackers, and criminals bent on turning the digital realm into a war zone. "In the battle raging between offense and defense in cyberspace, Clarke and Knake have some important ideas about how we can avoid cyberwar for our country, prevent cybercrime against our companies, and in doing so, reduce resentment, division, and instability at home and abroad."--Bill Clinton There is much to fear in the dark corners of cyberspace: we have entered an age in which online threats carry real-world consequences. But we do not have to let autocrats and criminals run amok in the digital realm. We now know a great deal about how to make cyberspace far less dangerous--and about how to defend our security, economy, democracy, and privacy from cyber attack. Our guides to the fifth domain -- the Pentagon's term for cyberspace -- are two of America's top cybersecurity experts, seasoned practitioners who are as familiar with the White House Situation Room as they are with Fortune 500 boardrooms. Richard A. Clarke and Robert K. Knake offer a vivid, engrossing tour of the often unfamiliar terrain of cyberspace, introducing us to the scientists, executives, and public servants who have learned through hard experience how government agencies and private firms can fend off cyber threats. With a focus on solutions over scaremongering, and backed by decades of high-level experience in the White House and the private sector, The Fifth Domain delivers a riveting, agenda-setting

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

insider look at what works in the struggle to avoid cyberwar.

Blockchain technology is defined as a decentralized system of distributed registers that are used to record data transactions on multiple computers. The reason this technology has gained popularity is that you can put any digital asset or transaction in the blocking chain, the industry does not matter. Blockchain technology has infiltrated all areas of our lives, from manufacturing to healthcare and beyond. Cybersecurity is an industry that has been significantly affected by this technology and may be more so in the future. Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications is an invaluable resource to discover the blockchain applications for cybersecurity and privacy. The purpose of this book is to improve the awareness of readers about blockchain technology applications for cybersecurity and privacy. This book focuses on the fundamentals, architectures, and challenges of adopting blockchain for cybersecurity. Readers will discover different applications of blockchain for cybersecurity in IoT and healthcare. The book also includes some case studies of the blockchain for e-commerce online payment, retention payment system, and digital forensics. The book offers comprehensive coverage of the most essential topics, including: Blockchain architectures and challenges Blockchain threats and vulnerabilities Blockchain security and potential future use cases Blockchain for securing Internet of Things Blockchain for cybersecurity in healthcare Blockchain in facilitating payment system security and privacy This book comprises a number of state-of-the-art contributions from both scientists and practitioners working in the fields of blockchain technology and cybersecurity. It aspires to provide a relevant reference for students, researchers, engineers, and professionals working in this particular area or those interested in grasping its diverse facets and exploring the latest advances on the blockchain for cybersecurity and privacy.

Risk-based operational audits and performance audits require a broad array of competencies. This book provides auditors and risk professionals with the understanding required to improve results during risk-based audits. Mastering the Five Tiers of Audit Competency: The Essence of Effective Auditing is an anthology of powerful risk-based auditing practices. Filled with practical do and don't techniques, it encompasses the interpersonal aspects of risk-based auditing, not just the technical content. This book details the behaviors you need to demonstrate and the habitual actions you need to take at each phase in an audit to manage the people relationships as well as the work itself. Each section of this book is devoted to a component of the audit: planning, detailed risk and control assessment, testing, audit report writing, project management, audit team management, and client relationship management. The book leverages The Whole Person Project, Inc.'s 30 years of hands-on organizational development experience and custom-designed internal audit training programs to aid those just starting out in audit as well as more experienced auditors. It also contains templates you can use to set performance goals and assess your progress towards achieving those goals. This book will spark ideas that can enhance performance, improve working relationships, and make it easier to complete audits that improve your organization's risk management culture and practices. Explaining how to make positive and sustained changes to the way you approach your work, the book includes a summary of the key points and a brief quiz to help you remember salient ideas in each chapter. Presenting proven methods and advice that can help you immediately save time, reduce stress, and produce reliable, quality results, this book is an ideal resource for anyone looking to make positive changes and adopt more productive work habits Use the guidance in this comprehensive field guide to gain the support of your top executives for aligning a rational cybersecurity plan with your business. You will learn how to improve working relationships with stakeholders in complex digital businesses, IT, and development environments. You will know how to prioritize your security program, and motivate and retain your team. Misalignment between security and your business can start at the top at the C-suite or happen at the line of business, IT, development, or user level. It has a corrosive effect on

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

any security project it touches. But it does not have to be like this. Author Dan Blum presents valuable lessons learned from interviews with over 70 security and business leaders. You will discover how to successfully solve issues related to: risk management, operational security, privacy protection, hybrid cloud management, security culture and user awareness, and communication challenges. This book presents six priority areas to focus on to maximize the effectiveness of your cybersecurity program: risk management, control baseline, security culture, IT rationalization, access control, and cyber-resilience. Common challenges and good practices are provided for businesses of different types and sizes. And more than 50 specific keys to alignment are included. What You Will Learn Improve your security culture: clarify security-related roles, communicate effectively to businesspeople, and hire, motivate, or retain outstanding security staff by creating a sense of efficacy Develop a consistent accountability model, information risk taxonomy, and risk management framework Adopt a security and risk governance model consistent with your business structure or culture, manage policy, and optimize security budgeting within the larger business unit and CIO organization IT spend Tailor a control baseline to your organization's maturity level, regulatory requirements, scale, circumstances, and critical assets Help CIOs, Chief Digital Officers, and other executives to develop an IT strategy for curating cloud solutions and reducing shadow IT, building up DevSecOps and Disciplined Agile, and more Balance access control and accountability approaches, leverage modern digital identity standards to improve digital relationships, and provide data governance and privacy-enhancing capabilities Plan for cyber-resilience: work with the SOC, IT, business groups, and external sources to coordinate incident response and to recover from outages and come back stronger Integrate your learnings from this book into a quick-hitting rational cybersecurity success plan Who This Book Is For Chief Information Security Officers (CISOs) and other heads of security, security directors and managers, security architects and project leads, and other team members providing security leadership to your business

With the rising cost of data breaches, executives need to understand the basics of cybersecurity so they can make strategic decisions that keep companies out of headlines and legal battles. Although top executives do not make the day-to-day technical decisions related to cybersecurity, they can direct the company from the top down to have a security mindset. As this book explains, executives can build systems and processes that track gaps and security problems while still allowing for innovation and achievement of business objectives. Many of the data breaches occurring today are the result of fundamental security problems, not crafty attacks by insidious malware. The way many companies are moving to cloud environments exacerbates these problems. However, cloud platforms can also help organizations reduce risk if organizations understand how to leverage their benefits. If and when a breach does happen, a company that has the appropriate metrics can more quickly pinpoint and correct the root cause. Over time, as organizations mature, they can fend off and identify advanced threats more effectively. The book covers cybersecurity fundamentals such as encryption, networking, data breaches, cyber-attacks, malware, viruses, incident handling, governance, risk management, security automation, vendor assessments, and cloud security.

RECOMMENDATION: As a former senior military leader, I learned early on that my personal expertise of a subject was less important than my ability to ask better questions of the experts. Often, I had no expertise at all but was required to make critical high risk decisions under very tight time constraints. In this book Teri helps us understand the better questions we should be asking about our data, data systems, networks, architecture development, vendors and cybersecurity writ large and why the answers to these questions matter to our organizations bottom line as well as our personal liability. Teri writes in a conversational tone adding personal experiences that bring life and ease of understanding to an otherwise very technical, complex and sometimes overwhelming subject. Each chapter breaks down a critical component that lends to a comprehensive understanding or can be taken individually. I am not steeped in cyber, but Teri's advice and recommendations

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

have proven critical to my own work on Boards of Directors as well as my leadership work with corporate CISOs, cybersecurity teams, and C-Suite executives. In a time-constrained world this is a worthy read. - Stephen A. Clark, Maj Gen, USAF (Ret) AUTHOR: Teri Radichel (@teriradichel) is the CEO of 2nd Sight Lab, a cloud and cybersecurity training and consulting company. She has a Master of Software Engineering, a Master of Information Security Engineering, and over 25 years of technology, security, and business experience. Her certifications include GSE, GXPN, GCIH, GPEN, GCIA, GCPM, GCCC, and GREM. SANS Institute gave her the 2017 Difference Makers Award for cybersecurity innovation. She is on the IANS (Institute for Applied Network Security) faculty and formerly taught and helped with curriculum for cloud security classes at SANS Institute. She is an AWS hero and runs the Seattle AWS Architects and Engineers Meetup which has over 3000 members. Teri was on the original Capital One cloud team helping with cloud engineering, operations, and security operations. She wrote a paper called Balancing Security and Innovation With Event Driven Automation based on lessons learned from that experience. It explains how companies can leverage automation to improve cybersecurity. She went on to help a security vendor move a product to AWS as a cloud architect and later Director of SaaS Engineering, where she led a team that implemented the concepts described in her paper. She now helps companies around the world with cloud and cyber security as a sought-after speaker, trainer, security researcher, and pentester.

Enhance your organization's secure posture by improving your attack and defense strategies Key Features Gain a clear understanding of the attack methods, and patterns to recognize abnormal behavior within your organization with Blue Team tactics. Learn to unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies. A practical guide that will give you hands-on experience to mitigate risks and prevent attackers from infiltrating your system. Book Description The book will start talking about the security posture before moving to Red Team tactics, where you will learn the basic syntax for the Windows and Linux tools that are commonly used to perform the necessary operations. You will also gain hands-on experience of using new Red Team techniques with powerful tools such as python and PowerShell, which will enable you to discover vulnerabilities in your system and how to exploit them. Moving on, you will learn how a system is usually compromised by adversaries, and how they hack user's identity, and the various tools used by the Red Team to find vulnerabilities in a system. In the next section, you will learn about the defense strategies followed by the Blue Team to enhance the overall security of a system. You will also learn about an in-depth strategy to ensure that there are security controls in each network layer, and how you can carry out the recovery process of a compromised system. Finally, you will learn how to create a vulnerability management strategy and the different techniques for manual log analysis. By the end of this book, you will be well-versed with Red Team and Blue Team techniques and will have learned the techniques used nowadays to attack and defend systems. What you will learn Learn the importance of having a solid foundation for your security posture Understand the attack strategy using cyber security kill chain Learn how to enhance your defense strategy by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligence Learn how to perform an incident investigation Get an in-depth understanding of the recovery process Understand continuous security monitoring and how to implement a vulnerability management strategy Learn how to perform log analysis to identify suspicious activities Who this book is for This book aims at IT professional who want to venture the IT security domain. IT pentester, Security consultants, and ethical hackers will also find this course useful. Prior knowledge of penetration testing would be beneficial. Exploring the negative social impact of cyber-attacks, this book takes a closer look at the challenges faced by both the public and private sectors of the financial industry. It is widely known amongst senior executives in both sectors that cybercrime poses a real threat, however

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

effective collaboration between individual financial institutions and the public sector into detecting, monitoring and responding to cyber-attacks remains limited. Addressing this problem, the authors present the results from a series of interviews with cybersecurity professionals based in Canada in order to better understand the potential risks and threats that financial institutions are facing in the digital age. Offering policy recommendations for improving cybersecurity protection measures within financial institutions, and enhancing the sharing of information between the public and private sector, this book is a timely and invaluable read for those researching financial services, cybercrime and risk management, as well as finance professionals interested in cybersecurity.

Managing Risk and Information Security: Protect to Enable, an ApressOpen title, describes the changing risk environment and why a fresh approach to information security is needed. Because almost every aspect of an enterprise is now dependent on technology, the focus of IT security must shift from locking down assets to enabling the business while managing and surviving risk. This compact book discusses business risk from a broader perspective, including privacy and regulatory considerations. It describes the increasing number of threats and vulnerabilities, but also offers strategies for developing solutions. These include discussions of how enterprises can take advantage of new and emerging technologies—such as social media and the huge proliferation of Internet-enabled devices—while minimizing risk. With ApressOpen, content is freely available through multiple online distribution channels and electronic formats with the goal of disseminating professionally edited and technically reviewed content to the worldwide community. Here are some of the responses from reviewers of this exceptional work: “Managing Risk and Information Security is a perceptive, balanced, and often thought-provoking exploration of evolving information risk and security challenges within a business context. Harkins clearly connects the needed, but often-overlooked linkage and dialog between the business and technical worlds and offers actionable strategies. The book contains eye-opening security insights that are easily understood, even by the curious layman.” Fred Wettling, Bechtel Fellow, IS&T Ethics & Compliance Officer, Bechtel “As disruptive technology innovations and escalating cyber threats continue to create enormous information security challenges, Managing Risk and Information Security: Protect to Enable provides a much-needed perspective. This book compels information security professionals to think differently about concepts of risk management in order to be more effective. The specific and practical guidance offers a fast-track formula for developing information security strategies which are lock-step with business priorities.” Laura Robinson, Principal, Robinson Insight Chair, Security for Business Innovation Council (SBIC) Program Director, Executive Security Action Forum (ESAF) “The mandate of the information security function is being completely rewritten. Unfortunately most heads of security haven’t picked up on the change, impeding their companies’ agility and ability to innovate. This book makes the case for why security needs to change, and shows how to get started. It will be regarded as marking the turning point in information security for years to come.” Dr. Jeremy Bergsman, Practice Manager, CEB “The world we are responsible to protect is changing dramatically and at an accelerating pace. Technology is pervasive in virtually every aspect of our lives. Clouds, virtualization and mobile are redefining computing – and they are just the beginning of what is to come. Your security perimeter is defined by wherever your information and people happen to be. We are attacked by professional adversaries who are better funded than we will ever be. We in the information security profession must change as dramatically as the environment we protect. We need new skills and new strategies to do our jobs effectively. We literally need to change the way we think. Written by one of the best in the business, Managing Risk and Information Security challenges traditional security theory with clear examples of the need for change. It also provides expert advice on how to dramatically increase the success of your security strategy and methods – from dealing with the misperception of risk to how to become a Z-shaped CISO. Managing Risk and Information Security is the ultimate treatise on how to deliver

Access Free Why Cisos Fail The Missing Link In Security Management And How To Fix It Internal Audit And It Audit

effective security to the world we live in for the next 10 years. It is absolute must reading for anyone in our profession – and should be on the desk of every CISO in the world.” Dave Cullinane, CISSP CEO Security Starfish, LLC “In this overview, Malcolm Harkins delivers an insightful survey of the trends, threats, and tactics shaping information risk and security. From regulatory compliance to psychology to the changing threat context, this work provides a compelling introduction to an important topic and trains helpful attention on the effects of changing technology and management practices.” Dr. Mariano-Florentino Cuéllar Professor, Stanford Law School Co-Director, Stanford Center for International Security and Cooperation (CISAC), Stanford University “Malcolm Harkins gets it. In his new book Malcolm outlines the major forces changing the information security risk landscape from a big picture perspective, and then goes on to offer effective methods of managing that risk from a practitioner's viewpoint. The combination makes this book unique and a must read for anyone interested in IT risk.” Dennis Devlin AVP, Information Security and Compliance, The George Washington University “Managing Risk and Information Security is the first-to-read, must-read book on information security for C-Suite executives. It is accessible, understandable and actionable. No sky-is-falling scare tactics, no techno-babble – just straight talk about a critically important subject. There is no better primer on the economics, ergonomics and psycho-behaviourals of security than this.” Thornton May, Futurist, Executive Director & Dean, IT Leadership Academy “Managing Risk and Information Security is a wake-up call for information security executives and a ray of light for business leaders. It equips organizations with the knowledge required to transform their security programs from a “culture of no” to one focused on agility, value and competitiveness. Unlike other publications, Malcolm provides clear and immediately applicable solutions to optimally balance the frequently opposing needs of risk reduction and business growth. This book should be required reading for anyone currently serving in, or seeking to achieve, the role of Chief Information Security Officer.” Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA “For too many years, business and security – either real or imagined – were at odds. In Managing Risk and Information Security: Protect to Enable, you get what you expect – real life practical ways to break logjams, have security actually enable business, and marries security architecture and business architecture. Why this book? It's written by a practitioner, and not just any practitioner, one of the leading minds in Security today.” John Stewart, Chief Security Officer, Cisco “This book is an invaluable guide to help security professionals address risk in new ways in this alarmingly fast changing environment. Packed with examples which makes it a pleasure to read, the book captures practical ways a forward thinking CISO can turn information security into a competitive advantage for their business. This book provides a new framework for managing risk in an entertaining and thought provoking way. This will change the way security professionals work with their business leaders, and help get products to market faster. The 6 irrefutable laws of information security should be on a stone plaque on the desk of every security professional.” Steven Proctor, VP, Audit & Risk Management, Flextronics

The book takes readers through a series of security and risk discussions based on real-life experiences. While the experience story may not be technical, it will relate specifically to a value or skill critical to being a successful CISO. The core content is organized into ten major chapters, each relating to a "Rule of Information Security" developed through a career of real life experiences. The elements are selected to accelerate the development of CISO skills critical to success. Each segments clearly calls out lessons learned and skills to be developed. The last segment of the book addresses presenting security to senior execs and board members, and provides sample content and materials.

[Copyright: a7448ce7a7efc761a8e9650905801cc9](https://www.cisohq.com/2017/05/14/why-cisos-fail-the-missing-link-in-security-management-and-how-to-fix-it-internal-audit-and-it-audit/)