

## Ciso Leadership Cyber Security Top Cop

*Divulging counterintuitive revelations about what it "really" takes to attract, develop, and retain top performers, this is the definitive guide to today's most urgent business dilemma.*

*CISO advice for communicating with the Board Of Directors about cybersecurity.*

*This book describes the thought process and specific activities a leader should consider as they interview for the IT risk/information security leader role, what they should do within their first 90 days, and how to organize, evangelize, and operate the program once they are into the job. Information technology (IT) risk and information security management are top of mind for corporate boards and senior business leaders. Continued intensity of cyber terrorism attacks, regulatory and compliance requirements, and customer privacy concerns are driving the need for a business-minded chief information security officer (CISO) to lead organizational efforts to protect critical infrastructure and sensitive data. A CISO must be able to both develop a practical program aligned with overall business goals and objectives and evangelize this plan with key stakeholders across the organization. The modern CISO cannot sit in a bunker somewhere in the IT operations center and expect to achieve buy in and support for the activities required to operate a program. This book describes the thought process and specific activities a leader should consider as they interview for the IT risk/information security leader role, what they should do within their first 90 days, and how to organize, evangelize, and operate the program once they are into the job. It provides practical, tested strategies for designing your program and guidance to help you be successful long term. It is chock full of examples, case studies, and diagrams right out of real corporate information security programs. The Business-Minded Chief Information Security Officer is a handbook for success as you begin this important position within any company.*

*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](http://www.mitre.org).*

*Managing Risk and Information Security*

*The Security Leader's Communication Playbook*

*A comprehensive guide to becoming a world-class modern cybersecurity leader and global CISO Well Aware*

*Fight Fire with Fire*

*Transforming Cybersecurity: Using COBIT 5*

*Network Security Strategies*

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.

Start your Cybersecurity career with expert advice on how to get certified, find your first job, and progress Key Features Learn how to follow your desired career path that results in a well-paid, rewarding job in cybersecurity Explore expert tips relating to career growth and certification options Access informative content from a panel of experienced cybersecurity experts Book Description Cybersecurity is an emerging career trend and will continue to become increasingly important. Despite the lucrative pay and significant career growth opportunities, many people are unsure of how to get started. This book is designed by leading industry experts to help you enter the world of cybersecurity with confidence, covering everything from gaining the right certification to tips and tools for finding your first job. The book starts by helping you gain a foundational understanding of cybersecurity, covering cyber law, cyber policy, and frameworks. Next, you'll focus on how to choose the career field best suited to you from options such as security operations, penetration testing, and risk analysis. The book also guides you through the different certification options as well as the pros and cons of a formal college education versus formal certificate courses. Later, you'll discover the importance of defining and understanding your brand. Finally, you'll get up to speed with different career paths and learning opportunities. By the end of this cyber book, you will have gained the knowledge you need to clearly define your career path and develop goals relating to career progression. What you will learn Gain an understanding of cybersecurity essentials, including the different frameworks and laws, and specialties Find out how to land your first job in the cybersecurity industry Understand the difference between college education and certificate courses Build goals

and timelines to encourage a work/life balance while delivering value in your job  
 Understand the different types of cybersecurity jobs available and what it means to be entry-level  
 Build affordable, practical labs to develop your technical skills  
 Discover how to set goals and maintain momentum after landing your first cybersecurity job  
 Who this book is for This book is for college graduates, military veterans transitioning from active service, individuals looking to make a mid-career switch, and aspiring IT professionals. Anyone who considers cybersecurity as a potential career field but feels intimidated, overwhelmed, or unsure of where to get started will also find this book useful. No experience or cybersecurity knowledge is needed to get started.

Organizations around the world are in a struggle for survival, racing to transform themselves in a herculean effort to adapt to the digital age, all while protecting themselves from headline-grabbing cybersecurity threats. As organizations succeed or fail, the centrality and importance of cybersecurity and the role of the CISO—Chief Information Security Officer—becomes ever more apparent. It's becoming clear that the CISO, which began as a largely technical role, has become nuanced, strategic, and a cross-functional leadership position. **Fight Fire with Fire: Proactive Cybersecurity Strategies for Today's Leaders** explores the evolution of the CISO's responsibilities and delivers a blueprint to effectively improve cybersecurity across an organization. **Fight Fire with Fire** draws on the deep experience of its many all-star contributors. For example: Learn how to talk effectively with the Board from engineer-turned-executive Marianne Bailey, a top spokesperson well-known for global leadership in cyber. Discover how to manage complex cyber supply chain risk with Terry Roberts, who addresses this complex area using cutting-edge technology and emerging standards. Tame the exploding IoT threat landscape with Sonia Arista, a CISO with decades of experience across sectors, including healthcare where edge devices monitor vital signs and robots perform surgery. These are just a few of the global trailblazers in cybersecurity who have banded together to equip today's leaders to protect their enterprises and inspire tomorrow's leaders to join them. With fires blazing on the horizon, there is no time for a seminar or boot camp. Cyber leaders need information at their fingertips. Readers will find insight on how to close the diversity and skills gap and become well-versed in modern cyber threats, including attacks coming from organized crime and nation-states. This book highlights a three-pronged approach that encompasses people, process, and technology to empower everyone to protect their organization. From effective risk management to supply chain security and communicating with the board, **Fight Fire with Fire** presents discussions from industry leaders that cover every critical competency in information security. Perfect for IT and information security professionals seeking perspectives and insights they can't find in certification exams or standard textbooks, **Fight Fire with Fire** is an indispensable resource for everyone hoping to improve their understanding of the realities of modern cybersecurity through the eyes of today's top security leaders.

Gain useful insights into cybersecurity leadership in a modern-day organization with the help of use cases  
 Key Features  
 Discover tips and expert advice from the leading CISO and author of many cybersecurity books  
 Become well-versed with a CISO's day-to-day responsibilities and learn how to perform them with ease  
 Understand real-world challenges faced by a CISO and find out the best way to solve them  
 Book Description The chief information security officer (CISO) is responsible for an organization's information and data security. The CISO's role is challenging as it demands a solid technical foundation as well as effective communication skills. This book is for busy cybersecurity leaders and executives looking to gain deep insights into the domains important for becoming a competent cybersecurity leader. The book begins by introducing you to the CISO's role, where you'll learn key definitions, explore the responsibilities involved, and understand how you can become an efficient CISO. You'll then be taken through end-to-end security operations and compliance standards to help you get to grips with the security landscape. In order to be a good leader, you'll need a good team. This book guides you in building your dream team by familiarizing you with HR management, documentation, and stakeholder onboarding. Despite taking all that care, you might still fall prey to cyber attacks; this book will show you how to quickly respond to an incident to help your organization minimize losses, decrease vulnerabilities, and rebuild services and processes. Finally, you'll explore other key CISO skills that'll help you communicate at both senior and operational levels. By the end of this book, you'll have gained a complete understanding of the CISO's role and be ready to advance your career. What you will learn  
 Understand the key requirements to become a successful CISO  
 Explore the cybersecurity landscape and get to grips with end-to-end security operations  
 Assimilate compliance standards, governance, and security frameworks  
 Find out how to hire the right talent and manage hiring procedures and budget  
 Document the approaches and processes for HR, compliance, and related domains  
 Familiarize yourself with incident response, disaster recovery, and business continuity  
 Get the hang of tasks and skills other than hardcore security operations  
 Who this book is for This book is for aspiring as well as existing CISOs. This book will also help cybersecurity leaders and security professionals understand leadership in this domain and motivate them to become leaders. A clear understanding of cybersecurity posture and a few years of experience as a cybersecurity professional will help you to get the most out of this book.

Protect to Enable

Cybersecurity ??? Attack and Defense Strategies

The Missing Link in Security Management--and How to Fix It

From the Boardroom to the Keyboard

The Perfect Scorecard

Cyber Mayday and the Day After

Rational Cybersecurity for Business

CYBER SECURITY will help you learn exactly what steps you, as a leader, can take to properly prepare your organization to face today's constantly evolving threat landscape. This book will help you not only understand the modern day threat landscape but also take action to ensure your company is safe.

Security practitioners must be able to build a cost-effective security program while at the same time meet the requirements of government regulations. This book lays out these regulations in simple terms and explains how to use the control framework to build an effective information security program and governance structure. It discusses how organizations can best ensure that the information is protected and examines all positions from the board of directors to the end user, delineating the role each plays in protecting the security of the organization.

An easy to use guide written by experienced practitioners for recently-hired or promoted Chief Information Security Officers (CISOs), individuals aspiring to become a CISO, as well as business and technical professionals interested in the topic of cybersecurity, including Chief Technology Officers (CTOs), Chief Information Officers (CIOs), Boards of Directors, Chief Privacy Officers, and other executives responsible for information protection. As a desk reference guide written specifically for CISOs, we hope this book becomes a trusted resource for you, your teams, and your colleagues in the C-suite. T

different perspectives can be used as standalone refreshers and the five immediate next steps for each chapter give a robust set of 45 actions based on roughly 100 years of relevant experience that will help you strengthen your cyber programs.

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

Cybersecurity Arm Wrestling

Winning the Perpetual Fight Against Crime by Building a Modern Security Operations Center (SOC)

Cyber Risk Leaders

Protecting Your Business from Real Threats in the Virtual World

Cybersecurity Leadership

Cybersecurity Career Master Plan

Navigating Cybersecurity Leadership Challenges with Insights from Pioneers

**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 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**

**Learn to effectively deliver business aligned cybersecurity outcomes In The CISO Evolution: Business Knowledge for Cybersecurity Executives, information security experts Matthew K. Sharp and Kyriakos "Rock" Lambros deliver an insightful and practical resource to help cybersecurity professionals develop the skills they need to effectively communicate with senior management and boards. They assert business aligned cybersecurity is crucial and demonstrate how business acumen is being put into action to deliver meaningful business outcomes. The authors use illustrative stories to show professionals how to establish an executive presence and avoid the most common pitfalls experienced by technology experts when speaking and presenting to executives. The book will show you how to: Inspire trust in senior business leaders by properly aligning and setting expectations around risk appetite and capital allocation Properly characterize the indispensable role of cybersecurity in your company's overall strategic plan Acquire the necessary funding and resources for your company's cybersecurity program and avoid the stress and anxiety that comes with underfunding Perfect for security and risk professionals, IT auditors, and risk managers looking for effective**

**strategies to communicate cybersecurity concepts and ideas to business professionals without a background in technology. The CISO Evolution is also a must-read resource for business executives, managers, and leaders hoping to improve the quality of dialogue with their cybersecurity leaders.**

**Widely acclaimed and cited by practitioners and scholars alike as the definitive book on cybersecurity leadership and governance appropriate for anyone within or outside the cybersecurity discipline. Explains cybersecurity, Chief Information Officer, Chief Information Security Officer roles, the role of ethical leadership and the need for perpetual innovation in the discipline. This is listed as one of the best books of all time in cybersecurity as well as management by BookAuthority. The book provides an authoritative peer reviewed definition of cybersecurity based on models explained in the books. It is a significant reference book for leadership in any organization; however, it specifically addresses the challenges unique to technology and cybersecurity. The book provides a business-level understanding of cybersecurity and critical leadership principles for interdisciplinary organizational leaders and technology professionals. It should be the starting point of anyone seeking to enter the cybersecurity field or gain a business level understanding of what is required for anyone to successfully implement cybersecurity in an organization.**

**The Psychology of Information Security – Resolving conflicts between security compliance and human behaviour considers information security from the seemingly opposing viewpoints of security professionals and end users to find the balance between security and productivity. It provides recommendations on aligning a security programme with wider organisational objectives, successfully managing change and improving security culture.**

**Cyber Crisis**

**Powering the Modern Organization**

**How to Succeed in InfoSec and Cybersecurity**

**Proactive Cybersecurity Strategies for Today's Leaders**

**Everything an Executive Needs to Know**

**Cybersecurity for Business**

**Cybersecurity Leadership Demystified**

*This book provides an advanced understanding of cyber threats as well as the risks companies are facing. It includes a detailed analysis of many technologies and approaches important to decreasing, mitigating or remediating those threats and risks. Cyber security technologies discussed in this book are futuristic and current. Advanced security topics such as secure remote work, data security, network security, application and device security, cloud security, and cyber risk and privacy are presented in this book. At the end of every chapter, an evaluation of the topic from a CISO's perspective is provided. This book also addresses quantum computing, artificial intelligence and machine learning for cyber security. The opening chapters describe the power and danger of quantum computing, proposing two solutions for protection from probable quantum computer attacks: the tactical enhancement of existing algorithms to make them quantum-resistant, and the strategic implementation of quantum-safe algorithms and cryptosystems. The following chapters make the case for using supervised and unsupervised AI/ML to develop predictive, prescriptive, cognitive and auto-reactive threat detection, mitigation, and remediation capabilities against advanced attacks perpetrated by sophisticated threat actors, APT and polymorphic/metamorphic malware. CISOs must be concerned about current on-going sophisticated cyber-attacks, and can address them with advanced security measures. The latter half of this book discusses some current sophisticated cyber-attacks and available protective measures enabled by the advancement of cybersecurity capabilities in various IT domains. Chapters 6-10 discuss secure remote work; chapters 11-17, advanced data security paradigms; chapters 18-28, Network Security; chapters 29-35, application and device security; chapters 36-39, Cloud security; and chapters 40-46 organizational cyber risk measurement and event probability. Security and IT engineers, administrators and developers, CIOs, CTOs, CISOs, and CFOs will want to purchase this book. Risk personnel, CROs, IT and Security Auditors as well as security researchers and journalists will also find this useful. The cost and frequency of cybersecurity incidents are on the rise, is your enterprise keeping pace? The numbers of threats, risk scenarios and vulnerabilities have grown exponentially. Cybersecurity has evolved as a new field of interest, gaining political and societal attention. Given this magnitude, the future tasks and responsibilities associated with cybersecurity will be essential to organizational survival and profitability. This publication applies the COBIT 5 framework and its component publications to transforming cybersecurity in a systemic way. First, the impacts of cybercrime and cyberwarfare on business and society are illustrated and put in context. This section shows the rise in cost and frequency of security incidents, including APT attacks and other threats with a critical impact and high intensity. Second, the transformation addresses security governance, security management and security assurance. In accordance with the lens concept within COBIT 5, these sections cover all elements of the systemic transformation and cybersecurity improvements.*

*Cyber Risk Leaders: Global C-Suite Insights - Leadership and Influence in the Cyber Age', by Shamane Tan - explores the art of communicating with executives, tips on navigating through corporate challenges, and reveals what the C-Suite looks for in professional partners. For those who are interested in learning from top industry leaders, or an aspiring or current CISO, this book is gold for your career. It's the go-to book and your CISO kit for the season.*

*The Security Hippie is Barak Engel's second book. As the originator of the "Virtual CISO" (fractional security chief) concept, he has served as security leader in dozens of notable organizations, such as Mulesoft, Stubhub, Amplitude Analytics, and many others. The Security Hippie follows his previous book, Why CISOs Fail, which became a sleeper hit, earning a spot in the Cybercannon project as a leading text on the topic of information security management. In this new book, Barak looks at security purely through the lens of story-telling, sharing many and varied experiences from his long and accomplished career as organizational and thought leader, and visionary in the information security field. Instead of instructing, this book teaches by example, sharing many real situations in the field and actual events from real companies, as well as Barak's related takes and thought processes. An out-of-the-mainstream, counterculture thinker – Hippie – in the world of information security, Barak's rich background and unusual approach to the field come forth in this book in vivid color and detail, allowing the reader to sit back and enjoy these experiences, and perhaps gain insights when faced with similar issues themselves or within their organizations. The author works hard to avoid technical terms as much as possible, and instead focus on the human and behavioral side of security, finding the humor inherent in every anecdote and using it to demystify the field and connect with the reader. Importantly, these are not the stories that made the news; yet they are the ones that happen all the time. If you've ever wondered about the field of information security, but have been intimidated by it, or simply wished for more shared experiences, then The Security Hippie is the perfect way to open that window by accompanying Barak on some of his many travels into the land of security.*

*Resolving conflicts between security compliance and human behaviour*

*Learn the art of human hacking with an internationally renowned expert*

*Best Practice Essentials with CISO/CSO Applications*

*Why CISOs Fail*

*The Security Hippie*

*Ten Strategies of a World-Class Cybersecurity Operations Center*

*Occupational Outlook Handbook*

Caught in the crosshairs of "Leadership" and "Information Technology", Information Security professionals are increasingly tapped to operate as business executives. This often puts them on a career path they did not expect, in a field not yet clearly defined. IT training does not usually includemanagerial skills such as leadership, team-building, communication, risk

assessment, and corporate business savvy, needed by CISOs. Yet a lack in any of these areas can short circuit a career in information security. CISO Leadership: Essential Principles for Success captures years of hard knocks, success stories, and yes, failures. This is not a how-to book or a collection of technical data. It does not cover products or technology or provide a recapitulation of the common body of knowledge. The book delineates information needed by security leaders and includes from-the-trenches advice on how to have a successful career in the field. With a stellar panel of contributors including William H. Murray, Harry Demaio, James Christiansen, Randy Sanovic, Mike Corby, Howard Schmidt, and other thought leaders, the book brings together the collective experience of trail blazers. The authors have learned through experience—been there, done that, have the t-shirt—and yes, the scars. A glance through the contents demonstrates the breadth and depth of coverage, not only in topics included but also in expertise provided by the chapter authors. They are the pioneers, who, while initially making it up as they went along, now provide the next generation of information security professionals with a guide to success.

Improve information security by learning Social Engineering. Key Features Learn to implement information security using social engineering Get hands-on experience of using different tools such as Kali Linux, the Social Engineering toolkit and so on Practical approach towards learning social engineering, for IT security Book Description This book will provide you with a holistic understanding of social engineering. It will help you to avoid and combat social engineering attacks by giving you a detailed insight into how a social engineer operates. Learn Social Engineering starts by giving you a grounding in the different types of social engineering attacks, and the damages they cause. It then sets up the lab environment to use different tools and then perform social engineering steps such as information gathering. The book covers topics from baiting, phishing, and spear phishing, to pretexting and scareware. By the end of the book, you will be in a position to protect yourself and your systems from social engineering threats and attacks. All in all, the book covers social engineering from A to Z, along with excerpts from many world wide known security experts. What you will learn Learn to implement information security using social engineering Learn social engineering for IT security Understand the role of social media in social engineering Get acquainted with Practical Human hacking skills Learn to think like a social engineer Learn to beat a social engineer Who this book is for This book targets security professionals, security analysts, penetration testers, or any stakeholder working with information security who wants to learn how to use social engineering techniques. Prior knowledge of Kali Linux is an added advantage

If you're a cybersecurity professional, then you know how it often seems that no one cares about (or understands) information security. InfoSec professionals frequently struggle to integrate security into their companies' processes. Many are at odds with their organizations. Most are under-resourced. There must be a better way. This essential manager's guide offers a new approach to building and maintaining an information security program that's both effective and easy to follow. Author and longtime chief information security officer (CISO) Todd Barnum upends the assumptions security professionals take for granted. CISOs, chief security officers, chief information officers, and IT security professionals will learn a simple seven-step process for building a new program or improving a current one. Build better relationships across the organization Align your role with your company's values, culture, and tolerance for information loss Lay the groundwork for your security program Create a communications program to share your team's contributions and educate your coworkers Transition security functions and responsibilities to other teams Organize and build an effective infosec team Measure your company's ability to recognize and report security policy violations and phishing emails The first section of this book addresses the evolution of CISO (chief information security officer) leadership, with the most mature CISOs combining strong business and technical leadership skills. CISOs can now add significant value when they possess an advanced understanding of cutting-edge security technologies to address the risks from the nearly universal operational dependence of enterprises on the cloud, the Internet, hybrid networks, and third-party technologies demonstrated in this book. In our new cyber threat-saturated world, CISOs have begun to show their market value. Wall Street is more likely to reward companies with good cybersecurity track records with higher stock valuations. To ensure that security is always a foremost concern in business decisions, CISOs should have a seat on corporate boards, and CISOs should be involved from beginning to end in the process of adopting enterprise technologies. The second and third sections of this book focus on building strong security teams, and exercising prudence in cybersecurity. CISOs can foster cultures of respect through careful consideration of the biases inherent in the socio-linguistic frameworks shaping our workplace language and through the cultivation of cyber exceptionalism. CISOs should leave no stone unturned in seeking out people with unique abilities, skills, and experience, and encourage career planning and development, in order to build and retain a strong talent pool. The lessons of the breach of physical security at the US Capitol, the hack back trend, and CISO legal liability stemming from network and data breaches all reveal the importance of good judgment and the necessity of taking proactive stances on preventative measures. This book will target security and IT engineers, administrators and developers, CIOs, CTOs, CISOs, and CFOs. Risk personnel, CROs, IT, security auditors and security researchers will also find this book

useful.

Organization-Wide Strategies to Ensure Cyber Risk Is Not Just an IT Issue

Modern Management and Leadership

Global CISO - Strategy, Tactics & Leadership

Learn Social Engineering

The CISO's Next Frontier

Cyber Security

A Leader's Guide to Preparing, Managing, and Recovering from the Inevitable

Successful, experienced, and award-winning Chief Information Security Officers and Risk Officers share their 'tips of the trade' with those who want to accelerate their paths in these fields. The combination of technical sophistication, fervent determination, and strong business acumen of this remarkable group, is what makes them excel consistently and against all odds. This is a 'must-read' for cyber and risk professionals that fulfill a daily crucial, global mission, and compete in one of the most intense careers in the world.

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 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.

Achieve digital transformation goals without creating undue risks with this guide to managing cybersecurity from a strategic, business-wide perspective.

As cyber security becomes the mainstay of businesses worldwide, it is imperative that leaders start developing the attitudes and the business acumen needed to manage risks and enable the business. This book provides a basic roadmap for information security leaders and those who aspire to be leaders on leading practices that are vital to the success of any organization that care about the security and privacy of their data and systems. This book provides leadership tenets that can be developed for Chief Information Security officers and those who aspire to be CISOs and also provides some basic guidelines on information security practices that help manage risk; from incident response and incident management to vulnerability management, security awareness and training, future trends in technology and security such as BYOD (bring you own device), cloud computing security, advanced persistent threats and many other information security leading practices and how to effectively manage and structure organizations for success against cyber attacks.

Security Leadership in a High Threat Landscape

Cybersecurity for Executives in the Age of Cloud

Information Security Governance Simplified

The War for Talent

## Pragmatic Advice for Emerging Risk Management Leaders

### The Security Leaders' Guide to Business Alignment

#### CISO Leadership

In one modest-sized volume, this book offers three valuable sets of knowledge. First, it provides best practice guidance on virtually every large-scale task a modern manager may be involved in—from recruiting and hiring to onboarding and leading teams, and from employee engagement and retention to performance management and working with difficult employees. Second, it explains the essential concepts and practice of a range of effective leadership styles—including (but not limited to) servant leadership, crisis leadership, change agent leadership, and diversity and inclusion leadership. Third, it offers brief case studies from select CISOs and CSOs on how these management and leadership principles and practices play out in real-life workplace situations. The best practice essentials provided throughout this volume will empower aspiring leaders and also enable experienced managers to take their leadership to the next level. Many if not most CISOs and other leaders have had very little, if any, formal training in management and leadership. The select few that have such training usually obtained it through academic courses that take a theoretical, broad brush approach. In contrast, this book provides much actionable guidance in the nitty-gritty tasks that managers must do every day. Lack of management practical knowledge puts CISOs and CSOs at a disadvantage vis-a-vis other executives in the C-suite. They risk being pigeonholed as “security cops” rather than respected business leaders. Many articles on these subjects published in the press are too incomplete and filled with bad information. And combing through the few high-quality sources that are out there, such as Harvard Business Publishing, can take hundreds of dollars in magazine subscription and book purchase fees and weeks or months of reading time. This book puts all the essential information into your hands through a series of concise chapters authored by an award-winning writer.

This book is written by a C(I)SO for C(I)SOs - and also addresses CEOs, CROs, CLOs, CIOs, CTOs, Security Managers, Privacy Leaders, Lawyers, and even Marketing and Sales executives. It is written by a seven-time career CISO for other visionaries, leaders, strategists, architects, compliance and audit experts, those politically interested, as well as, revolutionaries, and students of IS, IT, and STEM subjects that want to step up their game in InfoSec and Cybersecurity. The book connects the dots about past data breaches and their misconceptions; provides an international perspective on privacy laws like GDPR and several others, about threat actors and threat vectors; introduces strategy and tactics for securing your organization; presents a first glimpse on leadership; explains security program planning and backup plans; examines team building; conceptualizes the governance board; explores budgets; cooperates with the PMO; divulges into tactics; further elaborates on leadership; establishes the reporting structure; illustrates risk assessments; elucidates security processes, principals, and architectural designs; enumerates security metrics; skims compliance; demonstrates attack surface reduction; explicates security intelligence; conceptualizes S-SDLC (SecDevOps); depicts security management; epitomizes global leadership; illustrates the cloud's weaknesses; and finishes with an outlook on IoT. If you are in need of strong, proven, battle-tested security advice for a progressing security career, if you're looking for the security wisdom of a global, experienced leader to make smart decisions, if you are an architect and want to know how to securely architect and design using guiding principles, design patterns, and controls, or even if you work in sales and want to understand how (not) to sell to the CISO - this is your almanac - and you will read and reference it many times. 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.

This book is for cybersecurity leaders across all industries and organizations. It is intended to bridge the gap between the data center and the board room. This book examines the multitude of communication challenges that CISOs are faced with every day and provides practical tools to identify your audience, tailor your message and master the art of communicating. Poor communication is one of the top reasons that CISOs fail in their roles. By taking the step to work on your communication and soft skills (the two go hand-in-hand), you will hopefully never join their ranks. This is not a “communication theory” book. It provides just enough practical skills and techniques for security leaders to get the job done. Learn fundamental communication skills and how to apply them to day-to-day challenges like communicating with your peers, your team, business leaders and the board of directors. Learn how to produce meaningful metrics and communicate before, during and after an incident. Regardless of your role in Tech, you will find something of value somewhere along the way in this book.

#### The Business-Minded CISO

#### Essential Principles for Success

#### The Cybersecurity Manager's Guide

#### The CISO Mentor

#### Business Knowledge for Cybersecurity Executives

#### How to Organize, Evangelize, and Operate an Enterprise-wide IT Risk Management Program

#### A Practical Guide for CISOs

Practitioners in Cybersecurity community understand that they are in an unending war with opponents who have varying interests, but are mostly motivated by financial gains. New vulnerabilities are continuously discovered, new technologies are continuously being developed, and attackers are innovative in exploiting flaws to gain access to information assets for financial gains. It is profitable for attackers to succeed only few times. Security Operations Center (SOC) plays a key role in this perpetual arm wrestling to ensure you win most of the times. And if you fail once in a while, you can get back very quickly without much damage. People, who are part of SOC planning, architecture, design, implementation, operations, and incidents response will find this book useful. Many public and private sector organizations have built Security Operations Centers in-house whereas others have outsourced SOC operations to managed security services providers. Some also choose a hybrid approach by keeping parts of SOC operations in-house and outsourcing the rest of it. However, many of these efforts don't bring the intended results or realize desired business outcomes. This book is an effort to learn from experiences of many SOC practitioners and researchers to find practices that have been proven to be useful while avoiding common pitfalls in building SOC. I have also explored different ideas to find a "balanced" approach towards building a SOC and making informed choices between functions that can/should be kept in-house and the ones that can be outsourced. Even if you are an experienced SOC professional, you will still find few interesting ideas as I have done significant research and interviewed many SOC professionals to include tips to help avoid pitfalls.

Key Strategies to Safeguard Your Future Well Aware offers a timely take on the leadership issues that businesses face when it comes to the threat of hacking. Finney argues that cybersecurity is not a technology problem; it's a people problem. Cybersecurity should be understood as a series of nine habits

that should be mastered—literacy, skepticism, vigilance, secrecy, culture, diligence, community, mirroring, and deception—drawn from knowledge the author has acquired during two decades of experience in cybersecurity. By implementing these habits and changing our behaviors, we can combat most security problems. This book examines our security challenges using lessons learned from psychology, neuroscience, history, and economics. Business leaders will learn to harness effective cybersecurity techniques in their businesses as well as their everyday lives.

Examine the evolving enterprise security landscape and discover how to manage and survive risk. While based primarily on the author's experience and insights at major companies where he has served as CISO and CSPO, the book also includes many examples from other well-known companies and provides guidance for a management-level audience. *Managing Risk and Information Security* provides thought leadership in the increasingly important area of enterprise information risk and security. It 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 not only for internal operations but increasing as a part of product or service creation, the focus of IT security must shift from locking down assets to enabling the business while managing and surviving risk. This edition discusses business risk from a broader perspective, including privacy and regulatory considerations. It describes the increasing number of threats and vulnerabilities and 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. What You'll Learn Review how people perceive risk and the effects it has on information security See why different perceptions of risk within an organization matters Understand and reconcile these differing risk views Gain insights into how to safely enable the use of new technologies Who This Book Is For The primary audience is CIOs and other IT leaders, CISOs and other information security leaders, IT auditors, and other leaders of corporate governance and risk functions. The secondary audience is CEOs, board members, privacy professionals, and less senior-level information security and risk professionals. "Harkins' logical, methodical approach as a CISO to solving the most complex cybersecurity problems is reflected in the lucid style of this book. His enlightened approach to intelligence-based security infrastructure and risk mitigation is our best path forward if we are ever to realize the vast potential of the innovative digital world we are creating while reducing the threats to manageable levels. The author shines a light on that path in a comprehensive yet very readable way." —Art Coviello, Former CEO and Executive Chairman, RSA

*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 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

CISO COMPASS

The CISO's Transformation

Ciso Leadership

Protect your network and enterprise against advanced cybersecurity attacks and threats

Proven techniques and effective tips to help you advance in your cybersecurity career

Master the Nine Cybersecurity Habits to Protect Your Future

The CISO Evolution

**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.

Based on news reports, you might think there's a major cybersecurity threat every four to five months. In reality, there's a cybersecurity attack happening every minute of every day. Today, we live our lives—and conduct our business—online. Our data is in the cloud and in our pockets on our smartphones, shuttled over public Wi-Fi and company networks. To keep it safe, we rely on passwords and encryption and private servers, IT departments and best practices. But as you read this, there is a 70 percent chance that your data is compromised . . . you just don't know it yet. Cybersecurity attacks have increased exponentially, but because they're stealthy and often invisible, many underplay, ignore, or simply don't realize the danger. By the time they discover a breach, most individuals and businesses have been compromised for over three years. Instead of waiting until a problem surfaces, avoiding a data disaster means acting now to prevent one. In *Cyber Crisis*, Eric Cole gives readers a clear-eyed picture of the information war raging in cyberspace. Drawing on 30 years of experience—as a professional hacker for the CIA, as the Obama administration's cybersecurity commissioner, and as a consultant to clients around the globe from Bill Gates to Lockheed Martin and McAfee—Cole offers practical, actionable advice that even those with little technical background can implement, including steps to take on a daily, weekly, and monthly basis to protect their businesses and themselves. No matter who you are or where you work, cybersecurity should be a top priority. The information infrastructure we rely on in every sector of our lives—in healthcare and finance, for governments and private citizens—is both critical and vulnerable, and sooner or later, you or your company will be a target. This book is your guide to understanding the threat and putting together a proactive plan to minimize exposure and damage, and ensure the security of your business, your family, and your future

Digital transformation and cyber insecurity are two global trends that converged in 2020. The COVID-19 pandemic has accelerated these global challenges into paradigm-changing realities that threaten to destroy every company, government, network, and individual. But what can be done to embrace the accelerating digital disruption and at the same time manage the explosion of vulnerabilities, cyber threats, and business risks? What strategies are enabling technology leaders to thrive in this fast-changing landscape and stay calm in the midst of a world filled with ransomware, online deception, and nation-state hackers? *Cyber Mayday and the Day After* is a business book, a communication toolkit offering stories, strategies, tactics, and outlook with key extracts and lessons learned from top C-executive leaders around the world. Some of these insights come from former FBIs, NASA agents, government CISOs, and high profile CxOs, offering practical examples and workable solutions for leaders to succeed in the 21st century. This book unpacks key learnings on leadership and nfluence. It equips readers with the mastery of th r stakeholders and explores how to effect a cultural change within organizations.

**AI, Post-Quantum Cryptography and Advanced Security Paradigms**

**Infrastructure security with Red Team and Blue Team tactics**

**Getting an a in Cybersecurity from Your Board of Directors**

**Bridging the Gap between Security and the Business**

**The Psychology of Information Security**

**Cyber Security Top Cop**

**CISO Desk Reference Guide**