Security Risk Management Building An Information Security Risk Management Program From The Ground Up

Building a Travel Risk Management Program: Traveler Safety and Duty of Care for Any Organization helps business and security professionals effectively manage traveler risk by showing them how to build a complete travel risk program. While global corporate travel risks are increasing exponentially, many security and business managers are not well-versed in the rapidly changing global landscape of travel risk, nor do they fully realize the multitude of risks their companies face if they don't comply with their legal obligations—"duty of care"—for protecting their employees from foreseeable harm, which can cost a company in the form of extensive fines, productivity loss, business interruptions, stock price loss, litigation, and even potential bankruptcy. This book is the first to bridge the gap between the topics of travel management, security, and risk management. It serves as a reference point for working with other departments, including human resources and legal, paving the way for better internal cooperation for travel managers and security managers. In addition, it helps organizations craft a travel risk management program for their unique needs that incorporates the most important policies and procedures that help them comply with legal obligations. Illustrates common mistakes that can have a devastating impact across the entire enterprise with real-world examples and case studies Includes testimonies from corporate travel risk security experts on best practices for meeting the constantly changing duty of care standard Presents best practices for reducing the risk of exposure and liability Offers models for effectively promoting and advocating for travel risk management programs within the organization Compares laws like the UK s "Corporate Manslaughter Act (considered one of the world's most strict legislative standards) to similar laws around the world, showing how compliance requires constant supervision and process improvement

Is security management changing so fast that you can't keep up? Perhaps it seems like those traditional "best practices" in security no longer work? One answer might be that you need better best practices! In their new book, The Manager's Guide to Enterprise Security Risk Management: Essentials of Risk-Based Security, two experienced professionals introduce ESRM. Their practical, organization-wide, integrated approach redefines the securing of an organization's people and assets from being task-based to being risk-based. In their careers, the authors, Brian Allen and Rachelle Loyear, have been instrumental in successfully reorganizing the way security is handled in major corporations. In this ground-breaking book, the authors begin by defining Enterprise Security Risk Management (ESRM): "Enterprise security risk management is the application of fundamental risk principles to manage all security risks ? whether information, cyber, physical security, asset management, or business continuity ? in a comprehensive, holistic, all-encompassing approach." In the face of a continually evolving and increasingly risky global security landscape, this book takes you through the steps of putting ESRM into practice enterprise-wide, and helps you to: Differentiate between traditional, task-based management and strategic, risk-based management. See how adopting ESRM can lead to a more successful security program overall and enhance your own career. . Prepare your security organization to adopt an ESRM methodology. . Analyze and communicate risks and their root causes to all appropriate parties. . Identify what elements are necessary for long-term success of your ESRM program. . Ensure the proper governance of the security function in your enterprise. . Explain the value of security and ESRM to executives using useful metrics and reports. . Throughout the book, the authors provide a wealth of real-world case studies from a wide range of businesses and industries to help you overcome any blocks to acceptance as you design and roll out a new ESRM-based security program for your own workplace.

Enterprise Security Risk Management: Developing an Effective Asset Protection Program shows how to think about the underlying risks organizations face and how they connect to the threats and challenges in today's global environment. Security management in many organizations is often based on a reaction to the latest threat or a recent major loss. In contrast, this book advocates for an ongoing analytical and strategic process that responds to the ever changing risk environment, connecting practical applications to the real world challenges that all organizational and security professionals face daily. Offering a menu of strategies for success, Enterprise Security Risk Management provides the foundation with which both professionals and students can understand, build, and implement an effective asset protection program. Beginning with a conceptual overview of enterprise security risk management, the book explores the key tools that can be orchestrated into a comprehensive assets protection strategy. Covering applications and issues in a variety of organizational settings and industry sectors, the book draws a critical nexus between the security function and organizational management for any organization. Blends conceptual precepts with practical application, making it accessible for both real world and academic settings Illustrates key points using case studies Provides context with a "Setting the Stage" section at the start of each chapter Includes "Thought Exercises to challenge readers to identify how to they would respond to real-world scenarios Provides a "Digging Deeper" section with specific references and resources related to the topic in each chapter and section for further reading

Aware that a single crisis event can devastate their business, managers must be prepared for the worst from an expansive array of threats. The Routledge Companion to Risk, Crisis and Security in Business comprises a professional and scholarly collection of work in this critical field. Risks come in many varieties, and there is a growing concern for organizations to respond to the challenge. Businesses can be severely impacted by natural and man-made disasters including: floods, earthquakes, tsunami, environmental threats, terrorism, supply chain risks, pandemics, and white-collar crime. An organization's resilience is dependent not only on their own system security and infrastructure, but also on the wider infrastructure providing health and safety, utilities, transportation, and communication. Developments in risk security and management knowledge offer a path towards resilience and recovery through effective leadership in crisis situations. The growing body of knowledge in research and methodologies is a basis for decisions to safeguard people and assets, and to ensure the survivability of an organization from a crisis. Not only can businesses become more secure through risk management, but an effective program can also facilitate innovation and afford new opportunities. With chapters written by an international selection of leading experts, this book fills a crucial gap in our current knowledge of risk, crisis and security in business by exploring a broad spectrum of topics in the field. Edited by a globally-recognized expert on risk, this book is a vital reference for researchers, professionals and students with an interest in current scholarship in this expanding discipline.

An Interagency Approach to Creating Safe Facilities
Building an Information Security
Security Risk Management
Best Practices for Securing Infrastructure
Physical Security and Safety
The OCTAVE Approach
Lessons from Risk Management and Risk Assessment

Building a Practical Information Security Program provides users with a strategic view on how to build an information security program that aligns with business objectives. The information provided enables both executive management and IT managers not only to validate existing security programs, but also to build new business-driven security programs. In addition, the subject matter supports aspiring security engineers to forge a career path to successfully manage a security program, thereby adding value and reducing risk to the business. Readers learn how to translate technical challenges into business requirements, understand when to "go big or go home," explore in-depth defense strategies, and review tactics on when to absorb risks. This book explains how to properly plan and implement an infosec program based on business strategy and results. Provides a roadmap on how to build a security program that will protect companies from intrusion Shows how to focus the security program on its essential mission and move past FUD (fear, uncertainty, and doubt) to provide business value Teaches how to build consensus with an effective business-focused program

Information Security Policies, Procedures, and Standards: A Practitioner's Reference gives you a blueprint on how to develop effective information security policies and procedures. It uses standards such as NIST 800-53, ISO 27001, and COBIT, and regulations such as HIPAA and PCI DSS as the foundation for the content. Highlighting key terminology, policy development concepts and methods, and suggested document structures, it includes examples, checklists, sample policies and procedures, guidelines, and a synopsis of the applicable standards. The author explains how and why procedures are developed and implemented rather than simply provide information and examples. This is an important distinction because no two organizations are exactly alike; therefore, no two sets of policies and procedures are going to be exactly alike. This approach provides the foundation and understanding you need to write effective policies, procedures, and standards clearly and concisely. Developing policies and procedures may seem to be an overwhelming task. However, by relying on the material presented in this book, adopting the policy development techniques, and examining the examples, the task will not seem so daunting. You can use the discussion material to help sell the concepts, which may be the most difficult aspect of the process. Once you have completed a policy or two, you will have the courage to take on even more tasks. Additionally, the skills you acquire will assist you in other areas of your professional and private life, such as expressing an idea clearly and concisely or creating a project plan.

In order to protect company's information assets such as sensitive customer records, health care records, etc., the security practitioner first needs to find out: what needs protected, what risks those assets are exposed to, what controls are in place to offset those risks, and where to focus attention for risk treatment. This is the true value and purpose of information security risk assessments. Effective risk assessments are meant to provide a defendable analysis of residual risk associated with your key assets so that risk treatment options can be explored. Information Security Risk Assessments gives you the tools and skills to get a quick, reliable, and thorough risk assessment for key stakeholders. Based on authors' experiences of real-world assessments, reports, and presentations Focuses on implementing a process, rather than theory, that allows you to derive a quick and valuable assessment Includes a companion web site with spreadsheets you can utilize to create and maintain the risk assessment

This book provides a brief and general introduction to cybersecurity and cyber-risk assessment. Not limited to a specific approach or technique, its focus is highly pragmatic and is based on established international standards (including ISO 31000) as well as industrial best practices. It explains how cyber-risk assessment should be conducted, which techniques should be used when, what the typical challenges and problems are, and how they should be addressed. The content is divided into three parts. First, part I provides a conceptual introduction to the topic of risk management in general and to cybersecurity and cyber-risk management in particular. Next, part II presents the main stages of cyber-risk assessment from context establishment to risk treatment and acceptance, each illustrated by a running example. Finally, part III details four important challenges and how to reasonably deal with them in practice: risk measurement, risk scales, uncertainty, and low-frequency risks with high consequence. The target audience is mainly practitioners and students who are interested in the fundamentals and basic principles and techniques of security risk assessment, as well as lecturers seeking teaching material. The book provides an overview of the cyber-risk assessment process, the tasks involved, and how to complete them in practice.

Measuring and Managing Information Risk
Traveler Safety and Duty of Care for Any Organization
The Routledge Companion to Risk, Crisis and Security in Business
A FAIR Approach
Security Risk Assessment
Information Security Policies, Procedures, and Standards
Concepts and Applications

Effective risk management is essential for the success of large projects built and operated by the Department of Energy (DOE), particularly for the one-of-a-kind projects that characterize much of its mission. To enhance DOEâ€™s risk management efforts, the department asked the NRC to prepare a summary of the most effective practices used by leading owner organizations. The studyâ€™s primary objective was to provide DOE project managers with a basic understanding of both the project ownerâ€™s risk management role and effective oversight of those risk management activities delegated to contractors.

Written for people who manage information security risks for their organizations, this book details a security risk evaluation approach called "OCTAVE." The book provides a framework for systematically evaluating and managing security risks, illustrates the implementation of self-directed evaluations, and shows how to tailor evaluation methods to the needs of specific organizations. A running example illustrates key concepts and techniques. Evaluation worksheets and a catalog of best practices are included. The authors are on the technical staff of the Software Engineering Institute. Annotation copyrighted by Book News, Inc., Portland, OR

Follow step-by-step guidance to craft a successful security program. You will identify with the paradoxes of information security and discover handy tools that hook security controls into business processes. Information security is more than configuring firewalls, removing viruses, hacking machines, or setting passwords. Creating and promoting a successful security program requires skills in organizational consulting, diplomacy, change management, risk analysis, and out-of-the-box thinking. What You Will Learn: Build a security program that will fit neatly into an organization and change dynamically to suit both the needs of the organization and survive constantly changing threats Prepare for and pass such common audits as PCI-DSS, SSAE-16, and ISO 27001 Calibrate the scope, and customize security controls to fit into an organization's culture Implement the most challenging processes, pointing out common pitfalls and distractions Frame security and risk issues to be clear and actionable so that decision makers, technical personnel, and users will listen and value your advice Who This Book Is For: IT professionals moving into the security field; new security managers, directors, project heads, and would-be CISOs; and security specialists from other disciplines moving into information security (e.g., former military security professionals, law enforcement professionals, and physical security professionals)

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.

A Practical Guide
A Practical Introduction to Security and Risk Management
Managing Strategic Surprise
Best Practices for Building Security Risk Assessment and Management
The Palgrave Handbook of Security, Risk and Intelligence
Develop a threat model and incident response strategy to build a strong information security framework
The Craft of System Security

A framework for formalizing risk management thinking intoday¿s complex business environment Security Risk Management Body of Knowledge details thesecurity risk management process in a format that can easily beapplied by executive managers and security risk managementpractitioners. Integrating knowledge, competencies, methodologies,and applications, it demonstrates how to document and incorporatebest-practice concepts from a range of complementarydisciplines. Developed to align with International Standards for RiskManagement such as ISO 31000 it enables professionals to applysecurity risk management (SRM) principles to specific areas ofpractice. Guidelines are provided for: Access Management; BusinessContinuity and Resilience; Command, Control, and Communications;Consequence Management and Business Continuity Management;Counter-Terrorism; Crime Prevention through Environmental Design;Crisis Management; Environmental Security; Events and MassGatherings; Executive Protection; Explosives and Bomb Threats;Home-Based Work; Human Rights and Security; Implementing SecurityRisk Management; Intellectual Property Protection; IntelligenceApproach to SRM; Investigations and Root Cause Analysis; MaritimeSecurity and Piracy; Mass Transport Security; OrganizationalStructure; Pandemics; Personal Protective Practices; Psych-ology ofSecurity; Red Teaming and Scenario Modeling; Resilience andCritical Infrastructure Protection; Asset-, Function-, Project-,and Enterprise-Based Security Risk Assessment; SecuritySpecifications and Postures; Security Training; Supply ChainSecurity; Transnational Security; and Travel Security. Security Risk Management Body of Knowledge is supportedby a series of training courses, DVD seminars, tools, andtemplates. This is an indispensable resource for risk and securityprofessional, students, executive management, and line managerswith security responsibilities.

Practical guide that can be used by executives to make well-informed decisions on cybersecurity issues to better protect their business Emphasizes, in a direct and uncomplicated way, how executives can identify, understand, assess, and mitigate risks associated with cybersecurity issues Covers 'What to Do When You Get Hacked?' including Business Continuity and Disaster Recovery planning, Public Relations, Legal and Regulatory issues, and Notifications and Disclosures Provides steps for integrating cybersecurity into Strategy; Policy and Guidelines; Change Management and Personnel Management Identifies cybersecurity best practices that executives can and should use both in the office and at home to protect their vital information

Security Risk ManagementBuilding an Information Security Risk Management Program from the Ground UpElsevier

A practical and effective blueprint for world-class cybersecurity risk management In Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework, veteran technology analyst Cynthia Brumfield, with contributions from cybersecurity expert Brian Haugli, delivers a straightforward and up-to-date exploration of the fundamentals of cybersecurity risk planning and management. The book offers readers easy-to-understand overviews of cybersecurity risk management principles, user, and network infrastructure planning, as well as the tools and techniques for detecting cyberattacks. The book also provides a roadmap to the development of a continuity of operations plan in the event of a cyberattack. With incisive insights into the Framework for Improving Cybersecurity of Critical Infrastructure produced by the United States National Institute of Standards and Technology (NIST), Cybersecurity Risk Management presents the gold standard in practical guidance for the implementation of risk management best practices. Filled with clear and easy-to-follow advice, this book also offers readers: A concise introduction to the principles of cybersecurity risk management and the steps necessary to manage digital risk to systems, assets, data, and capabilities A valuable exploration of modern tools that can improve an organization's network infrastructure protection A practical discussion of the challenges involved in detecting and responding to a cyberattack and the importance of continuous security monitoring A helpful examination of the recovery from cybersecurity incidents Perfect for undergraduate and graduate students studying cybersecurity, Cybersecurity Risk Management is also an ideal resource for IT professionals working in private sector and government organizations worldwide who are considering implementing or who may be required to implement, the NIST framework at their organization.

Managing Risk and Information Security
How to Organize, Evangelize, and Operate an Enterprise-wide IT Risk Management Program
A Field Guide for the Practitioner
Security Risk Management Body of Knowledge
The Owner's Role in Project Risk Management
A Complete Guide for Performing Security Risk Assessments, Second Edition

Capitalist Nigger

This handbook provides a detailed analysis of threats and risk in the international system and of how governments and their intelligence services must adapt and function in order to manage the evolving security environment. This environment, now and for the foreseeable future, is characterised by complexity. The development of disruptive digital technologies; the vulnerability of critical national infrastructure; asymmetric threats such as terrorism; the privatisation of national intelligence capabilities: all have far reaching implications for security and risk management. The leading academics and practitioners who have contributed to this handbook have all done so with the objective of cutting through the complexity, and providing insight on the most pressing security, intelligence, and risk factors today. They explore the changing nature of conflict and crises; interaction of the global with the local; the impact of technological; the proliferation of hostile ideologies and the challenge this poses to traditional models of intelligence; and the impact of all these factors on governance and ethical frameworks. The handbook is an invaluable resource for students and professionals concerned with contemporary security and how national intelligence must adapt to remain effective.

How-To Guide Written By Practicing Professionals Physical Security and Safety: A Field Guide for the Practitioner introduces the basic principles of safety in the workplace, and effectively addresses the needs of the responsible security practitioner. This book provides essential knowledge on the procedures and processes needed for loss reduction, protection of organizational assets, and security and safety management. Presents Vital Information on Recognizing and Understanding Security Needs The book is divided into two parts. The first half of the text, Security and Safety Planning, explores the theory and concepts of security and covers: threat decomposition, identifying security threats and vulnerabilities, protection, and risk assessment. The second half, Infrastructure Protection, examines the overall physical protection program and covers: access and perimeter control, alarm systems, response force models, and practical considerations for protecting information technology (IT). Addresses general safety concerns and specific issues covered by Occupational Safety and Health Administration (OSHA) and fire protection regulations Discusses security policies and procedures required for implementing a system and developing an attitude of effective physical security Acts as a handbook for security applications and as a reference of security considerations Physical Security and Safety: A Field Guide for the Practitioner offers relevant discourse on physical security in the workplace, and provides a guide for security, risk management, and safety professionals.

Conducted properly, information security risk assessments provide managers with the feedback needed to manage risk through the understanding of threats to corporate assets, determination of current control vulnerabilities, and appropriate safeguards selection. Performed incorrectly, they can provide the false sense of security that allows potential threats to develop into disastrous losses of proprietary information, capital, and corporate value. Picking up where its bestselling predecessors left off, The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, Third Edition gives you detailed instruction on how to conduct a security risk assessment effectively and efficiently, supplying wide-ranging coverage that includes security risk analysis, mitigation, and risk assessment reporting. The third edition has expanded coverage of essential topics, such as threat analysis, data gathering, risk analysis, and risk assessment methods, and added coverage of new topics essential for current assessment projects (e.g., cloud security, supply chain management, and security risk assessment methods). This handbook walks you through the process of conducting an effective security assessment, and it provides the tools, methods, and up-to-date understanding you need to select the security measures best suited to your organization. Trusted to assess security for small companies, leading organizations, and government agencies, including the CIA, NSA, and NATO, Douglas J. Landoll unveils the little-known tips, tricks, and techniques used by savvy security professionals in the field. It includes features on how to Better negotiate the scope and rigor of security assessments Effectively interface with security assessment teams Gain an improved understanding of final report recommendations Deliver insightful comments on draft reports This edition includes detailed guidance on gathering data and analyzes over 200 administrative, technical, and physical controls using the RIIOT data gathering method; introduces the RIIOT FRAME (risk assessment method), including hundreds of tables, over 70 new diagrams and figures, and over 80 exercises; and provides a detailed analysis of many of the popular security risk assessment methods in use today. The companion website (infosecurityrisk.com) provides downloads for checklists, spreadsheets, figures, and tools.

Security Risk Assessment is the most up-to-date and comprehensive resource available on how to conduct a thorough security assessment for any organization. A good security assessment is a fact-finding process that determines an organization’s state of security protection. It exposes vulnerabilities, determines the potential for losses, and devises a plan to address these security concerns. While most security professionals have heard of a security assessment, many do not know how to conduct one, how it’s used, or how to evaluate what they have found. Security Risk Assessment offers security professionals step-by-step guidance for conducting a complete risk assessment. It provides a template draw from, giving security professionals the tools needed to conduct an assessment using the most current approaches, theories, and best practices. Discusses practical and proven techniques for effectively conducting security assessments Includes interview guides, checklists, and sample reports Accessibly written for security professionals with different levels of experience conducting security assessments

Managing Information Security Risks

Protect to Enable

Building a Travel Risk Management Program

Essentials of Risk-Based Security

The Security Risk Assessment Handbook

The Risk IT Practitioner Guide

Information Security Risk Assessment Toolkit

Though spectator and player security has always been a priority for sport and facility managers at all levels, large-scale threats such as terrorism or natural disasters have become even more critical management concerns. Proactive sport and facility managers understand the role they must take in working with local law enforcement, contracted security personnel, and their own employees to adequately plan for and respond to threats—both manmade and natural. Security Management for Sports and Special Events: An Interagency Approach to Creating Safe Facilities presents a systematic approach to stadium and venue security. Unlike traditional risk management books that present guidelines to promote safety and discourage litigation in sport and recreation settings, Security Management for Sports and SpecialEvents deals specifically with natural disasters, terrorism, crowd control problems, and other large-scale threats. As sport and facility managers seek to broaden their building management capabilities, this text offers detailed guidance in improving the quality, coordination, and responsiveness of security protocols within their facilities. With this text, sport and facility managers examine the concerns and challenges to security and emergency planning for both sport and non-sport events held at their facilities. Security Management for Sports and Special Events offers an organized explanation of event security to support the planning, implementation, and communication of security and emergency plans to staff and game-day hires as well as the assessment of emergency preparation. Drawing on numerous examples from both in and out of sport, readers will consider the challenges, solutions, best practices, and prescriptions for coordinating the efforts of staff, law enforcement, and security personnel. Readers will find an array of tools that assist in understanding and implementing the material presented: •Case studies at the end of each chapter and “Lessons Learned” sections that summarize and apply the information to a real-world scenario •Chapter goals and application questions that provide a clear map for the chapter and promote critical thinking of the issues •Sidebars throughout the text that provide examples of important current issues in sport and event security management •Reproducible checklists, forms, and additional resources that help in designing and implementing plans •More than 20 appendix items, including key guidelines, checklists, and needs assessments Emphasizing interagency development and a team approach to sport event security management, Security Managementfor Sports and Special Events allows sport and facility managers to lessen risk, control insurance costs, and uphold the integrity of their facilities through security management procedures. The text is developed according to the requirements of the Department of Homeland Security’s National Incident Management System (NIMS) and serves as the manual for managers seeking to achieve the SESA Seal of Approval offered by the University of Southern Mississippi’s National Center for Spectator Sports Safety and Security (NCS4). Developed by the authors and the only dedicated research facility for sport security management, NCS4 is on the cutting edge of researching and assessing game-day operations for security and crisis management. Security Management for Sports and Special Events is a practical resource for identifying and managing potential threats to fans’ and players’ safety. With proper protocols in place and a coordinated response, sport and facility professionals can ensure the safety of participants and spectators from terrorism, natural disasters, and other potential encounters.

A Practical Introduction to Security and Risk Management is the first book to introduce the full spectrum of security and risks and their management. Author and field expert Bruce Newsome helps readers learn how to understand, analyze, assess, control, and generally manage security and risks from the personal to the operational. They will develop the practical knowledge and skills they need, including analytical skills, basic mathematical methods for calculating risk in different ways, and more artistic skills in making judgments and decisions about which risks to control and how to control them. Organized into 16 brief chapters, the book shows readers how to: analyze security and risk; identify the sources of risk (including hazards, threats, and contributors); analyze exposure and vulnerability; assess uncertainty and probability; develop an organization’s culture, structure, and processes congruent with better security and risk management; choose different strategies for managing risks; communicate and review; and manage security in the key domains of operations, logistics, physical sites, information, communications, cyberspace, transport, and personal levels.

Best practices for protecting critical data and systems Information Assurance Handbook: Effective Computer Security and Risk Management Strategies discusses the tools and techniques required to prevent, detect, contain, correct, and recover from security breaches and other information assurance failures. This practical resource explains how to integrate information assurance into your enterprise planning in a non-technical manner. It leads you through building an IT strategy and offers an organizational approach to identifying, implementing, and controlling information assurance initiatives for small businesses and global enterprises alike. Common threats and vulnerabilities are described and applicable controls based on risk profiles are provided. Practical information assurance application examples are presented for select industries, including healthcare, retail, and industrial control systems. Chapter-ending critical thinking exercises reinforce the material covered. An extensive list of scholarly works and international government standards is also provided in this detailed guide. Comprehensive coverage includes: Basic information assurance principles and concepts Information assurance management system Current practices, regulations, and plans Impact of organizational structure Asset management Risk management and mitigation Human resource assurance Advantages of certification, accreditation, and assurance Information assurance in system development and acquisition Physical and environmental security controls Information assurance awareness, training, and education Access control Information security monitoring tools and methods Information assurance measurements and metrics Incident handling and computer forensics Business continuity management Backup and restoration Cloud computing and outsourcing strategies Information assurance big data concerns

Implement information security effectively as per your organization's needs. About This Book Learn to build your own information security framework, the best fit for your organization Build on the concepts of threat modeling, incidence response, and security analysis Practical use cases and best practices for information security Who This Book Is For This book is for security analysts and professionals who deal with security mechanisms in an organization. If you are looking for an end to end guide on information security and risk analysis with no prior knowledge of this domain, then this book is for you. What You Will Learn Develop your own information security framework Build your incident response mechanism Discover cloud security considerations Get to know the system development life cycle Get your security operation center up and running Know the various security testing types Balance security as per your business needs Implement information security best practices In Detail Having an information security mechanism is one of the most crucial factors for any organization. Important assets of organization demand a proper risk management and threat model for security, and so information security concepts are gaining a lot of traction. This book starts with the concept of information security and shows you why it's important. It then moves on to modules such as threat modeling, risk management, and mitigation. It also covers the concepts of incident response systems, information rights management, and more. Moving on, it guides you to build your own information security framework as the best fit for your organization. Toward the end, you'll discover some best practices that can be implemented to make your security framework strong. By the end of this book, you will be well-versed with all the factors involved in information security, which will help you build a security framework that is a perfect fit your organization's requirements. Style and approach This book takes a practical approach, walking you through information security fundamentals, along with information security best practices.

Cyber-Risk Management

The Road To Success - A Spider Web Doctrine

The Risk IT Framework

Mastering the Fundamentals using the NIST Cybersecurity Framework

The Manager’s Guide to Enterprise Security Risk Management

Cybersecurity for Executives

The Business-Minded CISCO

Proven set of best practices for security risk assessment and management, explained in plain English This guidebook sets forth a systematic, proven set of best practices for security risk assessment and management of buildings and their supporting infrastructures. These practices are all designed to optimize the security of workplace environments for occupants and to protect the interests of owners and other stakeholders. The methods set forth by the authors stem from their research at Sandia National Laboratories and their practical experience working with both government and private facilities. Following the authors' step-by-step methodology for performing a complete risk assessment, you learn to: Identify regional and site-specific threats that are likely and credible Evaluate the consequences of these threats, including loss of life and property, economic impact, as well as damage to symbolic value and public confidence Assess the effectiveness of physical and cyber security systems and determine site-specific vulnerabilities in the security system The authors further provide you with the analytical tools needed to determine whether to accept a calculated estimate of risk or to reduce the estimated risk to a level that meets your particular security needs. You then learn to implement a risk-reduction program through proven methods to upgrade security to protect against a malicious act and/or mitigate the consequences of the act. This comprehensive risk assessment and management approach has been used by various organizations, including the U.S. Bureau of Reclamation, the U.S. Army Corps of Engineers, the Bonneville Power Administration, and numerous private corporations, to assess and manage security risk at their national infrastructure facilities. With its plain-English presentation coupled with step-by-step procedures, flowcharts, worksheets, and checklists, you can easily implement the same proven approach and methods for your organization or clients. Additional forms and resources are available online at www.wiley.com/go/securityrisk.

The goal of Security Risk Management is to teach you practical techniques that will be used on a daily basis, while also explaining the fundamentals so you understand the rationale behind these practices. Security professionals often fall into the trap of telling the business that they need to fix something, but they can't explain why. This book will help you to break free from the so-called "best practices" argument by articulating risk exposures in business terms. You will learn techniques for how to perform risk assessments for new IT projects, how to efficiently manage daily risk activities, and how to qualify the current risk level for presentation to executive level management. While other books focus entirely on risk analysis methods, this is the first comprehensive guide for managing security risks.

Named a 2011 Best Governance and ISMS Book by InfoSec Reviews Includes case studies to provide hands-on experience using risk assessment tools to calculate the costs and benefits of any security investment Explores each phase of the risk management lifecycle, focusing on policies and assessment processes that should be used to properly assess and mitigate risk Presents a roadmap for designing and implementing a security risk management program

A ground shaking exposé on the failure of popular cyber risk management methods How to Measure Anything in Cybersecurity Risk exposes the shortcomings of current "risk management" practices, and offers a series of improvement techniques that help you fill the holes and ramp up security. In his bestselling book How to Measure Anything, author Douglas W. Hubbard opened the business world's eyes to the critical need for better measurement. This book expands upon that premise and draws from The Failure of Risk Management to sound the alarm in the cybersecurity realm. Some of the field's premier risk management approaches actually create more risk than they mitigate, and questionable methods have been duplicated across industries and embedded in the products accepted as gospel. This book sheds light on these blatant risks, and provides alternate techniques that can help improve your current situation. You'll also learn which approaches are too risky to save, and are actually more damaging than a total lack of any security. Dangerous risk management methods abound; there is no industry more critically in need of solutions than cybersecurity. This book provides solutions where they exist, and advises when to change tracks entirely. Discover the shortcomings of cybersecurity's "best practices" Learn which risk management approaches actually create risk Improve your current practices with practical alterations Learn which methods are beyond saving, and worse than doing nothing Insightful and enlightening, this book will inspire a closer examination of your company's own risk management practices in the context of cybersecurity. The end goal is airtight data protection, so finding cracks in the vault is a positive thing—as long as you get there before the bad guys do. How to Measure Anything in Cybersecurity Risk is your guide to more robust protection through better quantitative processes, approaches, and techniques.

Asks whether risk management techniques can be successfully applied to contemporary national security challenges.

IT Security Risk Control Management

A Structured Methodology

Assessing and Managing Security Risk in IT Systems

Information Assurance Handbook: Effective Computer Security and Risk Management Strategies

Cybersecurity Risk Management

Building an Information Security Risk Management Program from the Ground Up

As a security professional, have you found that you and others in your company do not always define “security” the same way? Perhaps security interests and business interests have become misaligned. Brian Allen and Rachelle Loyear offer a new approach: Enterprise Security Risk Management (ESRM). By viewing security through a risk management lens, ESRM can help make you and your security program successful. In their long-awaited book, based on years of practical experience and research, Brian Allen and Rachelle Loyear show you step-by-step how Enterprise Security Risk Management (ESRM) applies fundamental risk principles to manage all security risks. Whether the risks are informational, cyber, physical security, asset management, or business continuity, all are included in the holistic, all-encompassing ESRM approach which will move you from task-based to risk-based security. How is ESRM familiar? As a security professional, you may already practice some of the components of ESRM. Many of the concepts - such as risk identification, risk transfer and acceptance, crisis management, and incident response - will be well known to you. How is ESRM new? While many of the principles are familiar, the authors have identified few organizations that apply them in the comprehensive, holistic way that ESRM represents - and even fewer that communicate these principles effectively to key decision-makers. How is ESRM practical? ESRM offers you a straightforward, realistic, actionable approach to deal effectively with all the distinct types of security risks facing you as a security practitioner. ESRM is performed in a life cycle of risk management including: Asset assessment and prioritization. Risk assessment and prioritization. Risk treatment (mitigation). Continuous improvement. Throughout Enterprise Security Risk Management: Concepts and Applications, the authors give you the tools and materials that will help you advance you in the security field, no matter if you are a student, a newcomer, or a seasoned professional. Included are realistic case studies, questions to help you assess your own security program, thought-provoking discussion questions, useful figures and tables, and references for your further reading. By redefining how everyone thinks about the role of security in the enterprise, your security organization can focus on working in partnership with business leaders and other key stakeholders to identify and mitigate security risks. As you begin to use ESRM, following the instructions in this book, you will experience greater personal and professional satisfaction as a security professional - and you’ll become a recognized and trusted partner in the business-critical effort of protecting your enterprise and all its assets.

The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments provides detailed insight into precisely how to conduct an information security risk assessment. Designed for security professionals and their customers who want a more in-depth understanding of the risk assessment process, this volume contains real-wor

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

"I believe The Craft of System Security is one of the best software security books on the market today. It has not only breadth, but depth, covering topics ranging from cryptography, networking, and operating systems--to the Web, computer-human interaction, and how to improve the security of software systems by improving hardware. Bottom line, this book should be required reading for all who plan to call themselves security practitioners, and an invaluable part of every university's computer science curriculum." --Edward Bonver, CISSP, Senior Software QA Engineer, Product Security, Symantec Corporation "Here's to a fun, exciting read: a unique book chock-full of practical examples of the uses and the misuses of computer security. I expect that it will motivate a good number of college students to want to learn more about the field, at the same time that it will satisfy the more experienced professional." --L. Felipe Perrone, Department of Computer Science, Bucknell University Whether you're a security practitioner, developer, manager, or administrator, this book will give you the deep understanding necessary to meet today's security challenges--and anticipate tomorrow's. Unlike most books, The Craft of System Security doesn't just review the modern security practitioner's toolkit: It explains why each tool exists, and discusses how to use it to solve real problems. After quickly reviewing the history of computer security, the authors move on to discuss the modern landscape, showing how security challenges and responses have evolved, and offering a coherent framework for understanding today's systems and vulnerabilities. Next, they systematically introduce the basic building blocks for securing contemporary systems, apply those building blocks to today's applications, and consider important emerging trends such as hardware-based security. After reading this book, you will be able to Understand the classic Orange Book approach to security, and its limitations Use operating system security tools and structures--with examples from Windows, Linux, BSD, and Solaris Learn how networking, the Web, and wireless technologies affect security Identify software security defects, from buffer overflows to development process flaws Understand cryptographic primitives and their use in secure systems Use best practice techniques for authenticating people and computer systems in diverse settings Use validation, standards, and testing to enhance confidence in a system's security Discover the security, privacy, and trust issues arising from desktop productivity tools Understand digital rights management, watermarking, information hiding, and policy expression Learn principles of human-computer interaction (HCI) design for improved security Understand the potential of emerging work in hardware-based security and trusted computing

A Practitioner's Reference

An Audit Preparation Plan

How to Measure Anything in Cybersecurity Risk

Security Risk Assessment and Management

Practical Assessments Through Data Collection and Data Analysis

A Professional Practice Guide for Protecting Buildings and Infrastructures

Information Security Handbook

Despite the increase of high-profile hacks, record-breaking data leaks, and ransomware attacks, many organizations don't have the budget to establish or outsource an information security (InfoSec) program, forcing them to learn on the job. For companies obliged to improvise, this pragmatic guide provides a security-101 handbook with steps, tools, processes, and ideas to help you drive maximum-security improvement at little or no cost. Each chapter in this book provides step-by-step instructions for dealing with a specific issue, including breaches and disasters, compliance, network infrastructure and password management, vulnerability scanning, and penetration testing, among others. Network engineers, system administrators, and security professionals will learn tools and techniques to help improve security in sensible, manageable chunks. Learn fundamentals of starting or redesigning an InfoSec program Create a base set of policies, standards, and procedures Plan and design incident response, disaster recovery, compliance, and physical security Bolster Microsoft and Unix systems, network infrastructure, and password management Use segmentation practices and designs to compartmentalize your network Explore automated process and tools for vulnerability management Securely develop code to reduce exploitable errors Understand basic penetration testing concepts through purple teaming Delve into IDS, IPS, SOC, logging, and monitoring

Assessing and Managing Security Risk in IT Systems: A Structured Methodology builds upon the original McCumber Cube model to offer proven processes that do not change, even as technology evolves. This book enables you to assess the security attributes of any information system and implement vastly improved security environments. Part I delivers an overview of information systems security, providing historical perspectives and explaining how to determine the value of information. This section offers the basic underpinnings of information security and concludes with an overview of the risk management process. Part II describes the McCumber Cube, providing the original paper from 1991 and detailing ways to accurately map information flow in computer and telecom systems. It also explains how to apply the methodology to individual system components and subsystems. Part III serves as a resource for analysts and security practitioners who want access to more detailed information on technical vulnerabilities and risk assessment analytics. McCumber details how information extracted from this resource can be applied to his assessment processes.

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

Capitalist Nigger is an explosive and jarring indictment of the black race. The book asserts that the Negroid race, as naturally endowed as any other, is culpably a non-productive race, a consumer race that depends on other communities for its culture, its language, its feeding and its clothing. Despite enormous natural resources, blacks are economic slaves because they lack the "devil-may-care" attitude and the "killer instinct" of the Caucasian, as well as the spider web mentality of the Asian. A Capitalist Nigger must embody ruthlessness in pursuit of excellence in his drive towards achieving the goal of becoming an economic warrior. In putting forward the idea of the Capitalist Nigger, Chika Onyeani charts a road to success whereby black economic warriors employ the "Spider Web Doctrine" " discipline, self-reliance, ruthlessness " to escape from their victim mentality. Born in Nigeria, Chika Onyeani is a journalist, editor and former diplomat.

Building a World-Class Asset Protection Program

Enterprise Security Risk Management

Building a Practical Information Security Program

Managing Physical and Operational Security

Security Management for Sports and Special Events

A Complete Guide for Performing Security Risk Assessments

Defensive Security Handbook

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.