risk management, security management, cyber security, enterprise risk management, information security governance

Risk And Security Management

#risk management #security management #cyber security #enterprise risk management #information security governance

Effective risk and security management is crucial for modern enterprises, encompassing strategies to identify, assess, and mitigate potential threats. This discipline ensures robust cyber security and information security governance, protecting valuable assets and maintaining enterprise risk management frameworks. Implementing comprehensive security management practices safeguards against vulnerabilities and promotes business continuity.

Risk and Security Management

Learn to measure risk and develop a plan to protect employees and company interests by applying the advice and tools in Risk and Security Management: Protecting People and Sites Worldwide. In a world concerned with global terrorism, instability of emerging markets, and hazardous commercial operations, this book shines as a relevant and timely text with a plan you can easily apply to your organization. Find a series of strategic to granular level policies, systems, and concepts which identify and address risk, enabling business to occur in a manner which best protects you and your company.

A Practical Introduction to Security and Risk Management

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.

Risk, Crisis and Security Management

This book has two aims. First, it shows how risk, crisis and security, may be linked in an organisational context. Second, it reviews the role of simulation and gaming in responding to these phenomena. Issues of risk management are implicit in every debate about how social services such as health, transport and public safety are to be managed, and how corporate activity is to be regulated. This book informs that debate by considering the relationships between risk and security. Includes case studies such as the Kings Cross underground disaster, September 11, Hong Kong race track fire, and Arthur Anderson and the London ambulance computer failure.

Professional Security Management

Historically, security managers have tended to be sourced from either the armed forces or law enforcement. But the increasing complexity of the organisations employing them, along with the technologies employed by them, is forcing an evolution and expansion of the role, and security managers must meet this challenge in order to succeed in their field and protect the assets of their employers.
Risk management, crisis management, continuity management, strategic business operations, data security, IT, and business communications all fall under the purview of the security manager. This book is a guide to meeting those challenges, providing the security manager with the essential skill set and knowledge base to meet the challenges faced in contemporary, international, or tech-oriented businesses. It covers the basics of strategy, risk, and technology from the perspective of the security manager, focussing only on the 'need to know'. The reader will benefit from an understanding of how risk management aligns its functional aims with the strategic goals and operations of the organisation. This essential book supports professional vocational accreditation and qualifications, such as the Chartered Security Professional (CSyP) or Certified Protection Professional (CPP), and advises on pathways to higher education qualifications in the fields of security and risk management. It is ideal for any risk manager looking to further their training and development, as well as being complementary for risk and security management programs with a focus on practice.

Security Risk Management

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

People, Risk, and Security

Lance Wright shows why business in the 21st century requires a new understanding of the intersection of risk, security, and human resource management. He argues that these areas should no longer be considered separate processes, handled by technical specialists with limited spheres of expertise. People, risk and security management should be treated as a critically important integrated business management system. People may be your greatest asset – but they can also be your biggest liability. They expose you to all sorts of risks – risks from things they can do (or fail to do) and from things that can be done to them. No matter how tight a risk and security management policy may be in theory, it can fail on its first contact with reality if it doesn’t understand the people involved. Wright understands people, risk and security like few others. For years he was in charge people management for leading oil companies – getting people into and out of some of the most dangerous and hostile work environments on the planet – and keeping them safe while they were there. Then he was responsible for a private army, literally licenced to kill, guarding nuclear submarines that were being decommissioned as part of the Megatons to Megawatts program. Risk is more than a set of formulas. Security is more than guns, gates, and badges. Both ultimately come down to the people you are responsible for. One day, the depth of your understanding of that connection may what stands between you and disaster.

Security Risk Management Body of Knowledge

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.

Information Security Management

Information security cannot be effectively managed unless secure methods and standards are integrated into all phases of the information security life cycle. And, although the international community has been aggressively engaged in developing security standards for network and information security worldwide, there are few textbooks available that

Security Risk Management Body of Knowledge

A framework for formalizing risk management thinking in today¿s complex business environment Security Risk Management Body of Knowledge details the security risk management process in a format that can easily be applied by executive managers and security risk management practitioners. Integrating knowledge, competencies, methodologies, and applications, it demonstrates how to document and incorporate best-practice concepts from a range of complementary disciplines. Developed to align with International Standards for Risk Management such as ISO 31000 it enables professionals to apply security risk management (SRM) principles to specific areas of practice. Guidelines are provided for: Access Management; Business Continuity 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 Mass Gatherings; Executive Protection; Explosives and Bomb Threats; Home-Based Work; Human Rights and Security; Implementing Security Risk Management; Intellectual Property Protection; Intelligence Approach to SRM; Investigations and Root Cause Analysis; Maritime Security and Piracy; Mass Transport Security; Organizational Structure; Pandemics; Personal Protective Practices; Psych-ology of Security; Red Teaming and Scenario Modeling; Resilience and Critical Infrastructure Protection; Asset-, Function-, Project-, and Enterprise-Based Security Risk Assessment; Security Specifications and Postures; Security Training; Supply Chain Security; Transnational Security; and Travel Security. Security Risk Management Body of Knowledge is supported by a series of training courses, DVD seminars, tools, and templates. This is an indispensable resource for risk and security professional, students, executive management, and line managers with security responsibilities.

The Manager’s Guide to Enterprise Security Risk Management

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.

Cyber Security Management

Cyber Security Management: A Governance, Risk and Compliance Framework by Peter Trim and Yang-Im Lee has been written for a wide audience. Derived from research, it places security management in a holistic context and outlines how the strategic marketing approach can be used to underpin cyber security in partnership arrangements. The book is unique because it integrates material that is of a highly specialized nature but which can be interpreted by those with a non-specialist background in the area. Indeed, those with a limited knowledge of cyber security will be able to develop a comprehensive understanding of the subject and will be guided into devising and implementing relevant policy, systems and procedures that make the organization better able to withstand the increasingly sophisticated forms of cyber attack. The book includes a sequence-of-events model; an organizational governance framework; a business continuity management planning framework; a multi-cultural communication model; a cyber security management model and strategic management framework; an integrated governance mechanism; an integrated resilience management model; an integrated management model and system; a communication risk management strategy; and recommendations for counteracting a range of cyber threats. Cyber Security Management: A Governance, Risk and Compliance Framework simplifies complex material and provides a multi-disciplinary perspective and an explanation and interpretation of how managers can manage cyber threats in a pro-active manner and work towards counteracting cyber threats both now and in the future.

Security and Risk Management. Selected Academic Essays

Anthology from the year 2014 in the subject Business economics - Business Management, Corporate Governance, grade: 70%, University of Portsmouth (Institute of Criminal Justice Studies), course: BSc Security and Risk Management, language: English, abstract: This collection of essays outlines the work of one BSc student in Security and Risk Management from the University of Portsmouth, UK. It provides useful insights towards a better understanding of the topics of security, risk and organised crime. This book will be of particular relevance for BSc students in security and risk management and for security professionals who would like to deepen their academic knowledge. List of essays: What are the main influences on the function of a security manager in the retail and aviation sectors? Is there such a thing as an unified theory of risk and does the academic literature account for such principle adequately? There has been a move away from risk as probability to risk as accountability and liability which place the emphasis upon the individual Business continuity management has evolved as a business function Critically discuss how corporate security management is evolving The introduction of more privatisation into public policing will bring lower standards and risk greater corruption Critically examine the appropriateness of the term ‘organised crime’

Corporate Security Management

Corporate Security Management provides practical advice on efficiently and effectively protecting an organization's processes, tangible and intangible assets, and people. The book merges business and security perspectives to help transform this often conflicted relationship into a successful and sustainable partnership. It combines security doctrine, business priorities, and best practices to uniquely answer the Who, What, Where, Why, When and How of corporate security. Corporate Security Management explores the diverse structures of security organizations in different industries. It shows the crucial corporate security competencies needed and demonstrates how they blend with the competencies of the entire organization. This book shows how to identify, understand, evaluate and anticipate the specific risks that threaten enterprises and how to design successful protection strategies against them. It guides readers in developing a systematic approach to assessing, analyzing, planning, quantifying, administrating, and measuring the security function. Addresses the often opposing objectives between the security department and the rest of the business concerning risk, protection, outsourcing, and more Shows security managers how to develop business acumen in a corporate security environment Analyzes the management and communication skills needed for the corporate security manager Focuses on simplicity, logic and creativity instead of security technology Shows the true challenges of performing security in a profit-oriented environment, suggesting ways to successfully overcome them Illustrates the numerous security approaches and requirements in a wide variety of industries Includes case studies, glossary, chapter objectives, discussion questions and exercises

Information Security Management Metrics

Spectacular security failures continue to dominate the headlines despite huge increases in security budgets and ever-more draconian regulations. The 20/20 hindsight of audits is no longer an effective solution to security weaknesses, and the necessity for real-time strategic metrics has never been more critical. Information Security Management Metr

The Best Damn IT Security Management Book Period

The security field evolves rapidly becoming broader and more complex each year. The common thread tying the field together is the discipline of management. The Best Damn Security Manager's Handbook Period has comprehensive coverage of all management issues facing IT and security professionals and is an ideal resource for those dealing with a changing daily workload. Coverage includes Business Continuity, Disaster Recovery, Risk Assessment, Protection Assets, Project Management, Security Operations, and Security Management, and Security Design & Integration. Compiled from the best of the Syngress and Butterworth Heinemann libraries and authored by business continuity expert Susan Snedaker, this volume is an indispensable addition to a serious security professional's toolkit. * An all encompassing book, covering general security management issues and providing specific guidelines and checklists * Anyone studying for a security specific certification or ASIS certification will find this a valuable resource * The only book to cover all major IT and security management issues in one place: disaster recovery, project management, operations management, and risk assessment

Game Theory for Security and Risk Management

The chapters in this volume explore how various methods from game theory can be utilized to optimize security and risk-management strategies. Emphasizing the importance of connecting theory and practice, they detail the steps involved in selecting, adapting, and analyzing game-theoretic models in security engineering and provide case studies of successful implementations in different application domains. Practitioners who are not experts in game theory and are uncertain about incorporating it into their work will benefit from this resource, as well as researchers in applied mathematics and computer science interested in current developments and future directions. The first part of the book presents the theoretical basics, covering various different game-theoretic models related to and suitable for security engineering. The second part then shows how these models are adopted, implemented, and analyzed. Surveillance systems, interconnected networks, and power grids are among the different application areas discussed. Finally, in the third part, case studies from business and industry of successful applications of game-theoretic models are presented, and the range of applications discussed is expanded to include such areas as cloud computing, Internet of Things, and water utility networks.

Responsive Security

Responsive Security: Be Ready to Be Secure explores the challenges, issues, and dilemmas of managing information security risk, and introduces an approach for addressing concerns from both a practitioner and organizational management standpoint. Utilizing a research study generated from nearly a decade of action research and real-time experience, this book introduces the issues and dilemmas that fueled the study, discusses its key findings, and provides practical methods for managing information security risks. It presents the principles and methods of the responsive security approach, developed from the findings of the study, and details the research that led to the development of the approach. Demonstrates the viability and practicality of the approach in today's information security risk environment Demystifies information security risk management in practice, and reveals the limitations and inadequacies of current approaches Provides comprehensive coverage of the issues and challenges faced in managing information security risks today The author reviews existing literature that synthesizes current knowledge, supports the need for, and highlights the significance of the responsive security approach. He also highlights the concepts, strategies, and programs commonly used to achieve information security in organizations. Responsive Security: Be Ready to Be Secure examines the theories and knowledge in current literature, as well as the practices, related issues, and dilemmas experienced during the study. It discusses the reflexive analysis and interpretation involved in the final research cycles, and validates and refines the concepts, framework, and methodology of a responsive security approach for managing information security risk in a constantly changing risk environment.

Information Security Risk Management for ISO27001/ISO27002

Drawing on international best practice, including ISO/IEC 27005, NIST SP800-30 and BS7799-3, the book explains in practical detail how to carry out an information security risk assessment. It covers key topics, such as risk scales, threats and vulnerabilities, selection of controls, and roles and responsibilities, and includes advice on choosing risk assessment software.

Strategic Security Management

Strategic Security Management, Second Edition provides security leadership and decision-makers with a fresh perspective on threat, vulnerability, and risk assessment. The book offers a framework to look at applying security analysis and theory into practice for effective security program, implementation, management and evaluation. Chapters examine metric-based security resource allocation of countermeasures, including security procedures, utilization of personnel, and electronic measures. The new edition is fully updated to reflect the latest industry best-practices and includes contributions from security industry leaders—based on their years of professional experience—including: Nick Vellani, Michael Silva, Kenneth Wheatley, Robert Emery, Michael Haggard. Strategic Security Management, Second Edition will be a welcome addition to the security literature for all security professionals, security managers, and criminal justice students interested in understanding foundational security principles and their application.

Contemporary Security Management

SHORT BLURB/BRIEF DESCRIPTION: This is the third in a series of proposals for new editions of existing texts that have been adopted by DeVry University. In this case, the Keller Graduate School of Management at DeVry University has adopted Contemporary Security Management for their Master's Degree Program in Business Administration, Security Management concentration. It is at Keller's request that we update the material presented by John Fay in his original edition of the work. CONTEMPORARY SECURITY MANAGEMENT, 2e will be updated from the successful first edition which provides current, experience-proven business practices applicable to security operations. Vital topics covered include: managing in times of risk, target-hardening against terrorism, and strategies for cross-functional leadership. The author proposes he add two new chapters to cover terrorism and the new government mandate to perform standard vulnerability assessments for various industries. His outline of proposed changes is as follows: · The Terrorist Threat o International -- Al Qaeda; Hezbollah; Hamas; FLN; Sendero Luminoso; etc. o Domestic -- Aryan Nation; Animal Liberation Front; Environmental Liberation Front; etc. · Terrorist Motivations Political; Religious; Racial; Environmental; Special Interest · The Early Signals of Terrorism Target Surveillance; Information Collection; Tests of Security; Acquisition of Supplies; Dry Runs; Positioning to Act · Rating the Terrorist Group History; Current Configuration; Capabilities; Resolve; Target Preferences · Weapons of Major Concern Chemical; Biological; Radiological; Nuclear; Explosive; Incendiary · Vulnerability Factors Visibility of the Potential Target; Criticality of the Potential Target; Probability of Attack; Potential Consequences; Adversary Access and Proximity; Population Casualties; Collateral Damage · Vulnerability Assessment Models Generic; Industry Specific --Petroleum; Chemical; etc. · Vulnerabilities of Facilities Power; Water; Sewage; IT; HVAC · Special Targets Government Buildings; High-Impact Industrial Facilities; Financial Centers; Entertainment Venues; Schools; Hospitals; Food Supply Systems; Transportation Systems · Applicable Security Concepts All hazards and Design-Basis Analyses; Environmental Design; Stand-off Distance; Protection in Depth; Redundancy; Operations Security (OPSEC); Mitigation and remediation · Security Plan Development Gather and Analyze Data; Identify Critical Assets; Assess Current Protective Scheme; Identify Needs (Physical Security; Procedures; Manpower);; Write the Plan; Multidisciplinary Buy-In; Organize, Equip, and Train; Rehearse; Evaluate · Samples Vulnerability Assessment Checklist; Elements of a Security Plan; Department of Energy Best Practices Ancillary material: Instructor's Manual and Power Point Slides UNIQUE FEATURE: · An experience-proven, practical approach to the business of security · Author, John Fay, is very well known among security professionals and his sensible, down-to-earth style is accessible to those new to the business BENEFIT TO THE READER: · Case studies throughout the text provide real-world examples and solutions to management issues. · Samples of security plans and procedures, checklists, diagrams and illustrations aid in explaining a wide range of critical concepts

Encyclopedia of Security Management

The Encyclopedia of Security Management is a valuable guide for all security professionals, and an essential resource for those who need a reference work to support their continuing education. In keeping with the excellent standard set by the First Edition, the Second Edition is completely updated. The Second Edition also emphasizes topics not covered in the First Edition, particularly those relating to homeland security, terrorism, threats to national infrastructures (e.g., transportation, energy and agriculture) risk assessment, disaster mitigation and remediation, and weapons of mass destruction (chemical, biological, radiological, nuclear and explosives). Fay also maintains a strong focus on security measures required at special sites such as electric power, nuclear, gas and chemical plants; petroleum production and refining facilities; oil and gas pipelines; water treatment and distribution systems; bulk storage facilities; entertainment venues; apartment complexes and hotels; schools; hospitals; government buildings; and financial centers. The articles included in this edition also address protection of air, marine, rail, trucking and metropolitan transit systems. Completely updated to include new information concerning homeland security and disaster management Convenient new organization groups related articles for ease of use Brings together the work of more than sixty of the world's top security experts

Risk and the Theory of Security Risk Assessment

This book provides the conceptual foundation of security risk assessment and thereby enables reasoning about risk from first principles. It presents the underlying theory that is the basis of a rigorous and universally applicable security risk assessment methodology. Furthermore, the book identifies and explores concepts with profound operational implications that have traditionally been sources of ambiguity if not confusion in security risk management. Notably, the text provides a simple quantitative model for complexity, a significant driver of risk that is typically not addressed in security-related contexts. Risk and The Theory of Security Risk Assessment is a primer of security risk assessment pedagogy, but it also provides methods and metrics to actually estimate the magnitude of security risk. Concepts are explained using numerous examples, which are at times both enlightening and entertaining. As a result, the book bridges a longstanding gap between theory and practice, and therefore will be a useful reference to students, academics and security practitioners.

Risk Management for Security Professionals

This book describes the risk management methodology as a specific process, a theory, or a procedure for determining your assets, vulnerabilities, and threats and how security professionals can protect them. Risk Management for Security Professionals is a practical handbook for security managers who need to learn risk management skills. It goes beyond the physical security realm to encompass all risks to which a company may be exposed. Risk Management as presented in this book has several goals: Provides standardized common approach to risk management through a framework that effectively links security strategies and related costs to realistic threat assessment and risk levels Offers flexible yet structured framework that can be applied to the risk assessment and decision support process in support of your business or organization Increases awareness in terms of potential loss impacts, threats and vulnerabilities to organizational assets Ensures that various security recommendations are based on an integrated assessment of loss impacts, threats, vulnerabilities and resource constraints Risk management is essentially a process methodology that will provide a cost-benefit payback factor to senior management. Provides a stand-alone guide to the risk management process Helps security professionals learn the risk countermeasures and their pros and cons Addresses a systematic approach to logical decision-making about the allocation of scarce security resources

Cybersecurity Risk Management

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.

Enterprise risk & security management: everybody's business!.

Ideal for risk managers, information security managers, lead implementers, compliance managers and consultants, as well as providing useful background material for auditors, this book will enable readers to develop an ISO 27001-compliant risk assessment framework for their organisation and deliver real, bottom-line business benefits.

Information Security Risk Management for ISO 27001/ISO 27002, third edition

Flip This Risk® for Enterprise Security provides a holistic snapshot of select security management issues. It is a compilation of stories from experts in the field providingunique and creative perspectives on several security management areas including risk and resilience, business continuity, executive protection, GRC (Governance, Riskand Compliance), global monitoring, and travel and event security.In this book, our diversity of experts provides powerful narratives from personal and professional viewpoints, creating an opportunity for readers to easily grasp the concepts that frame security management in organizations. If you are seeking a better understanding of security management, desire additional knowledge about effective tools in the industry, or searching for leading practices that work in real-time-this book is for you!? Use it as a guide.? Use it as a reference.? Use it for inspiration.

Flip This Risk for Enterprise Security: Industry Experts Share Their Insights About Enterprise Security Management Risks for Organizations

How far would or should you go to feel secure? While everyone wants safety and security, the measures to achieve it are often viewed of as intrusive, unwanted, a hassle, and limiting to personal and professional freedoms. Yet, when an incident occurs, we can never have enough security. Security Management for Occupational Safety provides a framewor

Security Management for Occupational Safety

Risk Management for Computer Security provides IT professionals with an integrated plan to establish and implement a corporate risk assessment and management program. The book covers more than just the fundamental elements that make up a good risk program for computer security. It presents an integrated how-to approach to implementing a corporate program, complete with tested methods and processes, flowcharts, and checklists that can be used by the reader and immediately implemented into a computer and overall corporate security program. The challenges are many and this book will help professionals in meeting their challenges as we progress through the twenty-first century. This book is organized into five sections. Section I introduces the reader to the theories of risk management and describes the field's changing environment as well as the art of managing risks. Section II deals with threat assessment and its input to risk assessment; topics covered include the threat assessment method and an example of threat assessment. Section III focuses on operating system vulnerabilities and discusses application vulnerabilities; public domain vs. COTS; and connectivity and dependence. Section IV explains what risk assessment is and Section V explores qualitative vs. quantitative tools and types of risk assessment and concludes with an assessment of the future of risk management. Corporate security professionals around the world will find this book a highly valuable source of information. Presents material in an engaging, easy-to-follow manner that will appeal to both advanced INFOSEC career professionals and network administrators entering the information security profession Addresses the needs of both the individuals who are new to the subject as well as of experienced professionals Provides insight into the factors that need to be considered and fully explains the numerous methods, processes and procedures of risk management

Risk Management for Computer Security

Data processing, Computers, Management, Data security, Risk assessment, Data storage protection, Data, Information, Access, Anti-burglar measures, Organizations, Information exchange, Documents

Information Security Management Systems. Guidelines for Information Security Risk Management

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.

Enterprise Security Risk Management

Strategic Security Management supports data driven security that is measurable, quantifiable and practical. Written for security professionals and other professionals responsible for making security decisions as well as for security management and criminal justice students, this text provides a fresh perspective on the risk assessment process. It also provides food for thought on protecting an organization’s assets, giving decision makers the foundation needed to climb the next step up the corporate ladder. Strategic Security Management fills a definitive need for guidelines on security best practices. The book also explores the process of in-depth security analysis for decision making, and provides the reader with the framework needed to apply security concepts to specific scenarios. Advanced threat, vulnerability, and risk assessment techniques are presented as the basis for security strategies. These concepts are related back to establishing effective security programs, including program implementation, management, and evaluation. The book also covers metric-based security resource allocation of countermeasures, including security procedures, personnel, and electronic measures. Strategic Security Management contains contributions by many renowned security experts, such as Nick Vellani, Karl Langhorst, Brian Gouin, James Clark, Norman Bates, and Charles Sennewald. Provides clear direction on how to meet new business demands on the security professional Guides the security professional in using hard data to drive a security strategy, and follows through with the means to measure success of the program Covers threat assessment, vulnerability assessment, and risk assessment - and highlights the differences, advantages, and disadvantages of each

Strategic Security Management

Information risk management (IRM) is about identifying, assessing and prioritising risks to keep information secure and available. This accessible book provides practical guidance to the principles and development of a strategic approach to an IRM programme. The only textbook for the BCS Practitioner Certificate in Information Risk Management.

Information Risk Management

The guide covers the main processes involved in IT security management, based on ITIL and BSI best practice, and introduces a framework for IT security risk assessment and management. The guidelines are applicable to all IT organisations, irrespective of size or technology used, and can be adapted to fit each organisation individually based on its business, culture, structure, environment and processes.

IT Security Management

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.

Security Risk Assessment and Management

Security Culture starts from the premise that, even with good technical tools and security processes, an organisation is still vulnerable without a strong culture and a resilient set of behaviours in relation to people risk. Hilary Walton combines her research and her unique work portfolio to provide proven security culture strategies with practical advice on their implementation. And she does so across the board: from management buy-in, employee development and motivation, right through to effective metrics for security culture activities. There is still relatively little integrated and structured advice on how you can embed security in the culture of your organisation. Hilary draws all the best ideas together, including a blend of psychology, risk and security, to offer a security culture interventions toolkit from which you can pick and choose as you design your security culture programme - whether in private or public settings. Applying the techniques included in Security Culture will enable you to introduce or enhance a culture in which security messages stick, employees comply with policies, security complacency is challenged, and managers and employees understand the significance of this critically important, business-as-usual, function.

Security Culture

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

Security Risk Management

A comprehensive and practical guide to security organization and planning in industrial plants Features Basic definitions related to plant security Features Countermeasures and response methods Features Facilities and equipment, and security organization Topics covered are applicable to multiple types of industrial plants Illustrates practical techniques for assessing and evaluating financial and corporate risks

Industrial Security

Presents a system for crowd management which integrates security with the other concerns for the health and safety for crowds, looking at the theories and practices of the management processes, plans, monitoring and evaluation of crowds. Structured into four sections written by experts with global experience in their field of excellence.

Crowd Management

This new volume explores the crisis in transatlantic relations and analyses the role of NATO following the collapse of the Soviet Union. The book offers a unified theory of cooperation in the new security paradigm to explain the current state of transatlantic relations and NATO’s failure to adequately transform itself into a security institution for the 21st century. It argues that a new preoccupation with risk filled the vacuum left by the collapse of the Soviet Union, and uses the literature of the Risk Society to analyse the strained politics of the North Atlantic community. Using case studies to show how the West has pursued a strategy of risk management, and the effect this has had on NATO’s politics, the book argues that a better understanding of how risk affects Western political cohesion will allow policy makers a way of adapting the structure of NATO to make it more effective as a tool for security. Having analysed NATO’s recent failings, the book offers a theory for the way in which it can become an active risk manager, through the replacement of its established structure by smaller, ad hoc groupings.

NATO, Security and Risk Management