Management Of Information Security 3rd Edition

Eventually, you will totally discover a extra experience and skill by spending more cash. nevertheless when? complete you allow that you require to get those every needs once having significantly cash? Why dont you try to acquire something basic in the beginning? Thats something that will lead you to understand even more approaching the globe, experience, some places, taking into account history, amusement, and a lot more?

It is your enormously own era to deed reviewing habit. in the middle of guides you could enjoy now is **Management Of Information Security 3rd Edition** below.

Information Security and IT Risk Management - Manish Agrawal 2014-04-21
This new text provides students the knowledge and skills they will need to compete for and succeed in the information security roles they will encounter straight out of college. This is accomplished by providing a hands-on immersion in essential system administration, service and application installation and configuration, security tool use, TIG implementation and reporting. It is designed for an introductory course on IS Security offered usually as an elective in IS departments in 2 and 4 year schools. It is not designed for security certification courses.

The CIO's Guide to Information Security Incident Management - Matthew William Arthur Pemble 2018-10-26
This book will help IT and business operations managers who have been tasked with addressing security issues. It provides a solid understanding of security incident response and detailed guidance in the setting up and running of specialist incident management teams. Having an incident response plan is required for compliance with government regulations, industry standards such as PCI DSS, and certifications such as ISO 27001. This book will help organizations meet those compliance requirements.

Access Control and Identity Management - Mike Chapple 2020-10-01
Revised and updated with the latest data from this fast paced field, Access Control, Authentication, and Public Key Infrastructure defines the components of access control, provides a business framework for implementation, and discusses legal requirements that impact access control programs.

Managing Risk and Information Security - Malcolm Harkins 2013-03-21
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 Cu llar 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

Managing Information Security - John R. Vacca 2013-08-21

Managing Information Security offers focused coverage of how to protect mission critical systems, and how to deploy security management systems, IT security, ID management, intrusion detection and prevention systems, computer forensics, network forensics, firewalls, penetration testing, vulnerability assessment, and more. It offers in-depth coverage of the current technology and practice as it relates to information security management solutions. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. Chapters contributed by leaders in the field covering foundational and practical aspects of information security management, allowing the reader to develop a new level of technical expertise found nowhere else Comprehensive coverage by leading experts allows the reader to put current technologies to work Presents methods of analysis and problem solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Information Security Risk Analysis, Second Edition - Thomas R. Peltier 2005-04-26

The risk management process supports executive decision-making, allowing managers and owners to perform their fiduciary responsibility of protecting the assets of their enterprises. This crucial process should not be a long, drawn-out affair. To be effective, it must be done quickly and efficiently. Information Security Risk Analysis, Second Edition enables CIOs, CSOs, and MIS managers to understand when, why, and how risk assessments and analyses can be conducted effectively. This book discusses the principle of risk management and its three key elements: risk analysis, risk assessment, and vulnerability assessment. It examines the differences between quantitative and qualitative risk assessment, and details how various types of qualitative risk assessment can be applied to the assessment process. The text offers a thorough discussion of recent changes to FRAAP and the need to develop a pre-screening method for risk assessment and business impact analysis.

Fundamentals of Information Systems Security - David Kim 2016-10-15

Revised and updated with the latest data in the field, Fundamentals of Information Systems Security, Third Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transition to a digital world. Part 2 presents a high level overview of the Security+ Exam and provides students with information as they move toward this certification.

IT Security Risk Control Management - Raymond Pompon 2016-09-14

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)

Security Risk Management - Evan Wheeler 2011-04-20

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

Computer Security - ESORICS 94 - Dieter Gollmann 1994-10-19

This volume constitutes the proceedings of the Third European Symposium on Research in Computer Security, held in Brighton, UK in November 1994. The 26 papers presented in the book in revised versions were carefully selected from a total of 79 submissions; they cover many current aspects of computer security research and advanced applications. The papers are grouped in sections on high security assurance software, key management, authentication, digital payment, distributed systems, access control, databases, and measures.

Management of Information Security - Michael E. Whitman 2004

Designed for senior and graduate-level business and information systems students who want to learn the management aspects of information security, this work includes extensive end-of-chapter pedagogy to reinforce concepts as they are

learned.

Security Operations Management - Robert McCrie 2011-03-31

The second edition of Security Operations Management continues as the seminal reference on corporate security management operations. Revised and updated, topics covered in depth include: access control, selling the security budget upgrades to senior management, the evolution of security standards since 9/11, designing buildings to be safer from terrorism, improving relations between the public and private sectors, enhancing security measures during acute emergencies, and, finally, the increased security issues surrounding the threats of terrorism and cybercrime. An ideal reference for the professional, as well as a valuable teaching tool for the security student, the book includes discussion questions and a glossary of common security terms. Additionally, a brand new appendix contains contact information for academic, trade, and professional security organizations. * Fresh coverage of both the business and technical sides of security for the current corporate environment * Strategies for outsourcing security services and systems * Brand new appendix with contact information for trade, professional, and academic security organizations

Contemporary Security Management - David Patterson 2017-10-27

Contemporary Security Management, Fourth Edition, identifies and condenses into clear language the principal functions and responsibilities for security professionals in supervisory and managerial positions. Managers will learn to understand the mission of the corporate security department and how the mission intersects with the missions of other departments. The book assists managers with the critical interactions they will have with decision makers at all levels of an organization, keeping them aware of the many corporate rules, business laws, and protocols of the industry in which the corporation operates. Coverage includes the latest trends in ethics, interviewing, liability, and security-related standards. The book provides concise information on understanding budgeting, acquisition of capital equipment, employee performance rating, delegated authority, project management, counseling, and hiring. Productivity, protection of corporate assets, and monitoring of contract services and guard force operations are also detailed, as well as how to build quality relationships with leaders of external organizations, such as police, fire and emergency response agencies, and the Department of Homeland Security. Focuses on the evolving characteristics of major security threats confronting any organization Assists aspirants for senior security positions in matching their personal expertise and interests with particular areas of security management Includes updated information on the latest trends in ethics, interviewing, liability, and security-related standards

Healthcare Information Security and Privacy - Sean Murphy 2015-01-09

Secure and protect sensitive personal patient healthcare information Written by a healthcare information security and privacy expert, this definitive resource fully addresses security and privacy controls for patient healthcare information. Healthcare Information Security and Privacy introduces you to the realm of healthcare and patient health records with a complete overview of healthcare organization, technology, data, occupations, roles, and third parties. Learn best practices for healthcare information security and privacy with coverage of information governance, risk assessment and management, and incident response. Written for a global audience, this comprehensive guide covers U.S. laws and regulations as well as those within the European Union, Switzerland, and Canada. Healthcare Information and Security and Privacy covers: Healthcare industry Regulatory environment Privacy and security in healthcare Information governance Risk assessment and management

Fundamentals of Information Systems Security - David Kim 2013-07-11

PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Revised and updated with the latest information from this fast-paced field, Fundamentals of Information System Security, Second Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today. Part 2 is adapted from the Official (ISC)2 SSCP Certified Body of Knowledge and presents a high-level overview of each of the seven domains within the System Security Certified Practitioner certification. The book closes with a resource for readers who desire additional material on information security standards, education, professional certifications, and compliance laws. With its practical, conversational writing style and step-by-step examples, this text is a must-have resource for those entering the world of information systems security. New to the Second Edition: - New material on cloud computing, risk analysis, IP mobility, OMNIBus, and Agile Software Development. - Includes the most recent updates in Information Systems Security laws, certificates, standards, amendments, and the proposed Federal Information Security Amendments Act of 2013 and HITECH Act. - Provides new cases and examples pulled from real-world scenarios. - Updated data, tables, and sidebars provide the most current information in the field.

The Basics of Information Security - Jason Andress 2014-05-20

As part of the Syngress Basics series, The Basics of Information Security provides you with fundamental knowledge of information security in both theoretical and practical aspects. Author Jason Andress gives you the basic

knowledge needed to understand the key concepts of confidentiality, integrity, and availability, and then dives into practical applications of these ideas in the areas of operational, physical, network, application, and operating system security. The Basics of Information Security gives you clear-non-technical explanations of how infosec works and how to apply these principles whether you're in the IT field or want to understand how it affects your career and business. The new Second Edition has been updated for the latest trends and threats, including new material on many infosec subjects. Learn about information security without wading through a huge textbook Covers both theoretical and practical aspects of information security Provides a broad view of the information security field in a concise manner All-new Second Edition updated for the latest information security trends and threats, including material on incident response, social engineering, security awareness, risk management, and legal/regulatory issues

Readings and Cases in the Management of Information Security - Michael E. Whitman 2006

This text provides students with a set of industry focused readings and cases illustrating real-world issues in information security.

The InfoSec Handbook - Umesha Nayak 2014-09-17

The InfoSec Handbook offers the reader an organized layout of information that is easily read and understood. Allowing beginners to enter the field and understand the key concepts and ideas, while still keeping the experienced readers updated on topics and concepts. It is intended mainly for beginners to the field of information security, written in a way that makes it easy for them to understand the detailed content of the book. The book offers a practical and simple view of the security practices while still offering somewhat technical and detailed information relating to security. It helps the reader build a strong foundation of information, allowing them to move forward from the book with a larger knowledge base. Security is a constantly growing concern that everyone must deal with. Whether it's an average computer user or a highly skilled computer user, they are always confronted with different security risks. These risks range in danger and should always be dealt with accordingly. Unfortunately, not everyone is aware of the dangers or how to prevent them and this is where most of the issues arise in information technology (IT). When computer users do not take security into account many issues can arise from that like system compromises or loss of data and information. This is an obvious issue that is present with all computer users. This book is intended to educate the average and experienced user of what kinds of different security practices and standards exist. It will also cover how to manage security software and updates in order to be as protected as possible from all of the threats that they face.

Management of Information Security - Michael E. Whitman 2016-03-22

Readers discover a managerially-focused overview of information security with a thorough treatment of how to most effectively administer it with MANAGEMENT OF INFORMATION SECURITY, 5E. Information throughout helps readers become information security management practitioners able to secure systems and networks in a world where continuously emerging threats, ever-present attacks, and the success of criminals illustrate the weaknesses in current information technologies. Current and future professional managers complete this book with the exceptional blend of skills and experiences to develop and manage the more secure computing environments that today's organizations need. This edition offers a tightened focus on key executive and managerial aspects of information security while still emphasizing the important foundational material to reinforce key concepts. Updated content reflects the most recent developments in the field, including NIST, ISO, and security governance. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Information Security Management Principles - Andy Taylor 2019-10-31

In today's technology-driven environment, there is an ever-increasing demand for information delivery. A compromise has to be struck between security and availability. This book is a pragmatic guide to information assurance for both business professionals and technical experts. The third edition has been updated to reflect changes in the IT security landscape and updates to the BCS Certification in Information Security Management Principles, which the book supports.

Information Security Management Systems - Heru Susanto 2018-06-14

This new volume, Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standard, looks at information security management system standards, risk management associated with information security, and information security awareness within an organization. The authors aim to improve the overall ability of organizations to participate, forecast, and actively assess their information security circumstances. It is important to note that securing and keeping information from parties who do not have authorization to access such information is an extremely important issue. To address this issue, it is essential for an organization to implement an ISMS standard such as ISO 27001 to address the issue comprehensively. The authors of this new volume have constructed a novel security framework (ISF) and subsequently used this framework to develop software called Integrated Solution Modeling (ISM), a semi-automated system that will greatly help organizations comply with ISO 27001 faster and

cheaper than other existing methods. In addition, ISM does not only help organizations to assess their information security compliance with ISO 27001, but it can also be used as a monitoring tool, helping organizations monitor the security statuses of their information resources as well as monitor potential threats. ISM is developed to provide solutions to solve obstacles, difficulties, and expected challenges associated with literacy and governance of ISO 27001. It also functions to assess the RISC level of organizations towards compliance with ISO 27001. The information provide here will act as blueprints for managing information security within business organizations. It will allow users to compare and benchmark their own processes and practices against these results shown and come up with new, critical insights to aid them in information security standard (ISO 27001) adoption.

Information Security Handbook - Darren Death 2017-12-08

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.

Information Security Management Principles - Andy Taylor 2013

In todayOCOs technology-driven environment, there is an ever-increasing demand for information delivery. A compromise has to be struck between security and availability. This book is a pragmatic guide to information assurance for both business professionals and technical experts. This second edition includes the security of cloud-based resources."

Management of Information Security - Michael E. Whitman 2010-01-19

Management of Information Security, Third Edition focuses on the managerial aspects of information security and assurance. Topics covered include access control models, information security governance, and information security program assessment and metrics. Coverage on the foundational and technical components of information security is included to reinforce key concepts. This new edition includes up-to-date information on changes in the field such as revised sections on national and international laws and international standards like the ISO 27000 series. With these updates, Management of Information Security continues to offer a unique overview of information security from a management perspective while maintaining a finger on the pulse of industry changes and academic relevance. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Information Security - Mark Stamp 2005-11-11

Your expert guide to information security As businesses and consumers become more dependent on complexmultinational information systems, the need to understand anddevise sound information security systems has never been greater.This title takes a practical approach to information security byfocusing on real-world examples. While not sidestepping the theory,the emphasis is on developing the skills and knowledge thatsecurity and information technology students and professionals needto face their challenges. The book is organized around four majorthemes: * Cryptography: classic cryptosystems, symmetric key cryptography,public key cryptography, hash functions, random numbers,information hiding, and cryptanalysis * Access control: authentication and authorization, password-basedsecurity, ACLs and capabilities, multilevel and multilateralsecurity, covert channels and inference control, BLP and Biba'smodels, firewalls, and intrusion detection systems * Protocols: simple authentication protocols, session keys, perfectforward secrecy, timestamps, SSL, IPSec, Kerberos, and GSM * Software: flaws and malware, buffer overflows, viruses and worms,software reverse engineering, digital rights management, securesoftware development, and operating systems security Additional features include numerous figures and tables toillustrate and

clarify complex topics, as well as problems-rangingfrom basic to challenging-to help readers apply their newlydeveloped skills. A solutions manual and a set of classroom-testedPowerPoint(r) slides will assist instructors in their coursedevelopment. Students and professors in information technology,computer science, and engineering, and professionals working in thefield will find this reference most useful to solve theirinformation security issues. An Instructor's Manual presenting detailed solutions to all theproblems in the book is available from the Wiley editorialdepartment. An Instructor Support FTP site is also available.

Readings & Cases in Information Security: Law & Ethics - Michael E. Whitman 2010-06-23

Readings and Cases in Information Security: Law and Ethics provides a depth of content and analytical viewpoint not found in many other books. Designed for use with any Cengage Learning security text, this resource offers readers a real-life view of information security management, including the ethical and legal issues associated with various on-the-job experiences. Included are a wide selection of foundational readings and scenarios from a variety of experts to give the reader the most realistic perspective of a career in information security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The Economics of Information Security and Privacy - Rainer B hme 2013-11-29

In the late 1990s, researchers began to grasp that the roots of many information security failures can be better explained with the language of economics than by pointing to instances of technical flaws. This led to a thriving new interdisciplinary research field combining economic and engineering insights, measurement approaches and methodologies to ask fundamental questions concerning the viability of a free and open information society. While economics and information security comprise the nucleus of an academic movement that quickly drew the attention of thinktanks, industry, and governments, the field has expanded to surrounding areas such as management of information security, privacy, and, more recently, cybercrime, all studied from an interdisciplinary angle by combining methods from microeconomics, econometrics, qualitative social sciences, behavioral sciences, and experimental economics. This book is structured in four parts, reflecting the main areas: management of information security, economics of information security, economics of privacy, and economics of cybercrime. Each individual contribution documents, discusses, and advances the state of the art concerning its specific research questions. It will be of value to academics and practitioners in the related fields.

Management of Information Security, Loose-Leaf Version - Michael E. Whitman 2018-05-09

MANAGEMENT OF INFORMATION SECURITY, Sixth Edition prepares you to become an information security management practitioner able to secure systems and networks in a world where continuously emerging threats, ever-present attacks and the success of criminals illustrate the weaknesses in current information technologies. You'll develop both the information security skills and practical experience that organizations are looking for as they strive to ensure more secure computing environments. The text focuses on key executive and managerial aspects of information security. It also integrates coverage of CISSP and CISM throughout to effectively prepare you for certification. Reflecting the most recent developments in the field, it includes the latest information on NIST, ISO and security governance as well as emerging concerns like Ransomware, Cloud Computing and the Internet of Things.

Handbook of System Safety and Security - Edward Griffor 2016-10-02

Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Adversary Modeling, Threat Analysis, Business of Safety, Functional Safety, Software Systems, and Cyber Physical Systems presents an update on the world's increasing adoption of computer-enabled products and the essential services they provide to our daily lives. The tailoring of these products and services to our personal preferences is expected and made possible by intelligence that is enabled by communication between them. Ensuring that the systems of these connected products operate safely, without creating hazards to us and those around us, is the focus of this book, which presents the central topics of current research and practice in systems safety and security as it relates to applications within transportation, energy, and the medical sciences. Each chapter is authored by one of the leading contributors to the current research and development on the topic. The perspective of this book is unique, as it takes the two topics, systems safety and systems security, as inextricably intertwined. Each is driven by concern about the hazards associated with a system's performance. Presents the most current and leading edge research on system safety and security, featuring a panel of top experts in the field Includes several research advancements published for the first time, including the use of 'goal structured notation' together with a 'judgment calculus' and their automation as a 'rule set' to facilitate systems safety and systems security process execution in compliance with existing standards Presents for the first time the latest research in the field with the unique perspective that systems safety and systems security are inextricably intertwined Includes coverage of systems architecture, cyber physical systems, tradeoffs between safety, security, and performance, as well as the current methodologies and technologies and implantation practices for system safety and security

Cyber Security Awareness for CEOs and Management - David Willson

2015-12-09

Cyber Security for CEOs and Managment is a concise overview of the security threats posed to organizations and networks by the ubiquity of USB Flash Drives used as storage devices. The book will provide an overview of the cyber threat to you, your business, your livelihood, and discuss what you need to do, especially as CEOs and Management, to lower risk, reduce or eliminate liability, and protect reputation all related to information security, data protection and data breaches. The purpose of this book is to discuss the risk and threats to company information, customer information, as well as the company itself; how to lower the risk of a breach, reduce the associated liability, react quickly, protect customer information and the company's reputation, as well as discuss your ethical, fiduciary and legal obligations. Presents most current threats posed to CEOs and Managment teams. Offer detection and defense techniques

Cyber Security Management - Peter Trim 2016-05-13

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.

Legal Issues in Information Security - Grama 2014-08-12

Part of the Jones & Bartlett Learning Information Systems Security and Assurance Series http://www.issaseries.com Revised and updated to address the many changes in this evolving field, the Second Edition of Legal Issues in Information Security (Textbook with Lab Manual) addresses the area where law and information security concerns intersect. Information systems security and legal compliance are now required to protect critical governmental and corporate infrastructure, intellectual property created by individuals and organizations alike, and information that individuals believe should be protected from unreasonable intrusion. Organizations must build numerous information security and privacy responses into their daily operations to protect the business itself, fully meet legal requirements, and to meet the expectations of employees and customers. Instructor Materials for Legal Issues in Information Security include: PowerPoint Lecture Slides Instructor's Guide Sample Course Syllabus Quiz & Exam Questions Case Scenarios/Handouts New to the Second Edition: • Includes discussions of amendments in several relevant federal and state laws and regulations since 2011 • Reviews relevant court decisions that have come to light since the publication of the first edition • Includes numerous information security data breaches highlighting new vulnerabilities

Principles of Information Security - Michael E. Whitman 2014-11-26

Specifically oriented to the needs of information systems students, PRINCIPLES OF INFORMATION SECURITY, 5e delivers the latest technology and developments from the field. Taking a managerial approach, this bestseller teaches all the aspects of information security-not just the technical control perspective. It provides a broad review of the entire field of information security, background on many related elements, and enough detail to facilitate understanding of the topic. It covers the terminology of the field, the history of the discipline, and an overview of how to manage an information security program. Current and relevant, the fifth edition includes the latest practices, fresh examples, updated material on technical security controls, emerging legislative issues, new coverage of digital forensics, and hands-on application of ethical issues in IS security. It is the ultimate resource for future business decision-makers. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Elementary Information Security - Richard E. Smith 2013

Comprehensive and accessible, Elementary Information Security covers the entire range of topics required for US government courseware certification NSTISSI 4013 and urges students analyze a variety of security problems while gaining experience with basic tools of the trade. Written for the one-term undergraduate course, the text emphasises both the technical and non-technical aspects of information security and uses practical examples and real-world assessment tools. Early chapters in the text discuss individual computers and small LANS, while later chapters deal with distributed site security and the Internet. Cryptographic topics follow the same progression, starting on a single computer and evolving to Internet-level connectivity. Mathematical concepts

throughout the text are defined and tutorials with mathematical tools are provided to ensure students grasp the information at hand. Rather than emphasizing memorization, this text challenges students to learn how to analyze a variety of security problems and gain experience with the basic tools of this growing trade.Key Features:-Covers all topics required by the US government curriculum standard NSTISSI 4013.- Unlike other texts on the topic, the author goes beyond defining the math concepts and provides students with tutorials and practice with mathematical tools, making the text appropriate for a broad range of readers.- Problem Definitions describe a practical situation that includes a security dilemma.- Technology Introductions provide a practical explanation of security technology to be used in the specific chapters- Implementation Examples show the technology being used to enforce the security policy at hand- Residual Risks describe the limitations to the technology and illustrate various tasks against it.- Each chapter includes worked examples of techniques students will need to be successful in the course. For instance, there will be numerous examples of how to calculate the number of attempts needed to crack secret information in particular formats; PINs, passwords and encryption keys.

NETWORK SECURITY AND MANAGEMENT - BRIJENDRA SINGH 2011-12-24

Written in an easy-to-understand style, this textbook, now in its third edition, continues to discuss in detail important concepts and major developments in network security and management. It is designed for a one-semester course for undergraduate students of Computer Science, Information Technology, and undergraduate and postgraduate students of Computer Applications. Students are first exposed to network security principles, organizational policy and security infrastructure, and then drawn into some of the deeper issues of cryptographic algorithms and protocols underlying network security applications. Encryption methods, secret key and public key cryptography, digital signature and other security mechanisms are emphasized. Smart card, biometrics, virtual private networks, trusted operating systems, pretty good privacy, database security, and intrusion detection systems are comprehensively covered. An in-depth analysis of technical issues involved in security management, risk management and security and law is presented. In the third edition, two new chapters—one on Information Systems Security and the other on Web Security—and many new sections such as digital signature, Kerberos, public key infrastructure, software security and electronic mail security have been included. Additional matter has also been added in many existing sections. KEY FEATURES : Extensive use of block diagrams throughout helps explain and clarify the concepts discussed. About 250 questions and answers at the end of the book facilitate fruitful revision of the topics covered. Includes a glossary of important terms. KEY FEATURES : Extensive use of block diagrams throughout helps explain and clarify the concepts discussed. About 250 questions and answers at the end of the book facilitate fruitful revision of the topics covered. Includes a glossary of important terms.

Information Security Analytics - Mark Talabis 2014-11-25

Information Security Analytics gives you insights into the practice of analytics and, more importantly, how you can utilize analytic techniques to identify trends and outliers that may not be possible to identify using traditional security analysis techniques. Information Security Analytics dispels the myth that analytics within the information security domain is limited to just security incident and event management systems and basic network analysis. Analytic techniques can help you mine data and identify patterns and relationships in any form of security data. Using the techniques covered in this book, you will be able to gain security insights into unstructured big data of any type. The authors of Information Security Analytics bring a wealth of analytics experience to demonstrate practical, hands-on techniques through case studies and using freely-available tools that will allow you to find anomalies and outliers by combining disparate data sets. They also teach you everything you need to know about threat simulation techniques and how to use analytics as a powerful decision-making tool to assess security control and process requirements within your organization. Ultimately, you will learn how to use these simulation techniques to help predict and profile potential risks to your organization. Written by security practitioners, for security practitioners Real-world case studies and scenarios are provided for each analytics technique Learn about open-source analytics and statistical packages, tools, and applications Step-by-step guidance on how to use analytics tools and how they map to the techniques and scenarios provided Learn how to design and utilize simulations for "what-if" scenarios to simulate security events and processes Learn how to utilize big data techniques to assist in incident response and intrusion analysis

Information Security Management Handbook, Sixth Edition - Richard O'Hanley 2013-08-29

Updated annually, the Information Security Management Handbook, Sixth Edition, Volume 7 is the most comprehensive and up-to-date reference available on information security and assurance. Bringing together the knowledge, skills, techniques, and tools required of IT security professionals, it facilitates the up-to-date understanding required to stay one step ahead of evolving threats, standards, and regulations. Reporting on the latest developments in information security and recent changes to the (ISC)2® CISSP Common Body of Knowledge (CBK®), this volume features 27 new chapters on topics such as BYOD, IT consumerization, smart grids, security, and privacy. Covers the fundamental

knowledge, skills, techniques, and tools required by IT security professionals Updates its bestselling predecessors with new developments in information security and the (ISC)2® CISSP® CBK® Provides valuable insights from leaders in the field on the theory and practice of computer security technology Facilitates the comprehensive and up-to-date understanding you need to stay fully informed The ubiquitous nature of computers and networks will always provide the opportunity and means to do harm. This edition updates its popular predecessors with the information you need to address the vulnerabilities created by recent innovations such as cloud computing, mobile banking, digital wallets, and near-field communications. This handbook is also available on CD.

Principles of Information Security - Michael E. Whitman 2021-07-06

Discover the latest trends, developments and technology in information security today with Whitman/Mattord's market-leading PRINCIPLES OF INFORMATION SECURITY, 7th Edition. Designed specifically to meet the needs of those studying information systems, this edition's balanced focus addresses all aspects of information security, rather than simply offering a technical control perspective. This overview explores important terms and examines what is needed to manage an effective information security program. A new module details incident response and detection strategies. In addition, current, relevant updates highlight the latest practices in security operations as well as legislative issues, information management toolsets and digital forensics. Coverage of the most recent policies and guidelines that correspond to federal and international standards further prepare you for success both in information systems and as a business decision-maker. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Information Security Risk Management for ISO 27001/ISO 27002, third edition - Alan Calder 2019-08-29

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 ISO27001/ISO27002 - Alan Calder 2010-04-27

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.