Bodyguard Training Powerpoint Presentations

Understanding Personal Security and Risk
Evaluation and Management Coding and Documentation Guide
People Management
Practical Aviation Security
Information Security Governance Simplified
Careers in School Safety
Loss Control Auditing
Network and System Security
Secure Software Design
SSCP (ISC)2 Systems Security Certified Practitioner Official Study Guide
Physical Security for IT
Ensuring Information Assets Protection
Bodyguards
Cybersecurity for Executives
Modern Operatives
CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide
The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-601)
Building a Practical Information Security Program
CASP CompTIA Advanced Security Practitioner Study Guide
Making Sense of Cybersecurity
Sm Computers I/M
The Security Development Lifecycle
HIPAA Desk Reference 2003
Secrets Stolen, Fortunes Lost
Investigation of Management Problems at Los Alamos National Laboratory
Bringing a Corporate Security Culture to Life
HCI for Cybersecurity, Privacy and Trust
Men in Black
Security Operations Management
Well Aware
Basic Security Management
AIDCO Marketing - 5 Steps to Business Success
CASP: CompTIA Advanced Security Practitioner Study Guide Authorized Courseware
Strategic Security
Ensuring Information Assets Protection
Establishing Cyber Security Programs Through the Community Cyber Security Maturity Model (CCSMM)
Network and System Security
Computer and Information Security Handbook
Beyond the Bodyguard
HotelBusiness

KENNEDY DEACON

Understanding Personal Security and Risk Routledge
Your customers demand and deserve better security and privacy in their software. This book is the first to detail a rigorous, proven methodology that measurably minimizes security bugs--the Security Development Lifecycle (SDL). In this long-awaited book, security experts Michael Howard and Steve Lipner from the Microsoft Security Engineering Team guide you through each stage of the SDL--from education and design to testing and post-release. You get their first-hand insights, best practices, a practical history of the SDL, and lessons to help you implement the SDL in any development organization. Discover how to: Use a streamlined risk-analysis process to find security design issues before code is committed Apply secure-coding best practices and a proven testing process Conduct a final security review before a product ships Arm customers with prescriptive guidance to configure and deploy your product more securely Establish a plan to respond to new security vulnerabilities Integrate security discipline into agile methods and processes, such as Extreme Programming and Scrum Includes a CD featuring: A six-part security class video conducted by the authors and other Microsoft security experts Sample SDL documents and fuzz testing tool PLUS--Get book updates on the Web. For customers who purchase an ebook version of this title, instructions for downloading the CD files can be found in the ebook.
Evaluation and Management Coding and Documentation Guide Delmar
The second edition of Practical Aviation Security is a complete guide to the aviation security system, from crucial historical events to the policies, policymakers, and major terrorist and criminal acts that have shaped the procedures in use today. The tip-of-the-spear technologies that are shaping the future are also addressed. This text equips readers in airport security or other aviation management roles with the knowledge to implement the effective security programs, to meet international guidelines, and to responsibly protect facilities or organizations of any size. Using case studies and practical security measures now in use at airports worldwide, readers learn the effective methods and the fundamental principles involved in designing and implementing a security system. The aviation security system is comprehensive and requires continual focus and attention to stay a step ahead of the next attack. Practical Aviation Security, Second Edition helps prepare practitioners to enter the industry, and helps seasoned professionals prepare for new threats and prevent new tragedies. Covers commercial airport security, general aviation and cargo operations, threats, and threat detection and response systems, as well as international security issues Lays out the security fundamentals that can ensure the future of global travel and commerce Applies real-world aviation experience to the task of anticipating and deflecting threats
People Management John Wiley & Sons
Get Prepared for CompTIA Advanced Security Practitioner (CASP) Exam Targeting security professionals who either have their CompTIA Security+ certification or are looking to achieve a more advanced security certification, this CompTIA Authorized study guide is focused on the new CompTIA Advanced Security Practitioner (CASP) Exam CAS-001. Veteran IT security expert and author Michael Gregg details the technical knowledge and skills you need to conceptualize, design, and engineer secure solutions across complex enterprise environments. He prepares you for

aspects of the certification test that assess how well you apply critical thinking and judgment across a broad spectrum of security disciplines. Featuring clear and concise information on crucial security topics, this study guide includes examples and insights drawn from real-world experience to help you not only prepare for the exam, but also your career. You will get complete coverage of exam objectives for all topic areas including: Securing Enterprise-level Infrastructures Conducting Risk Management Assessment Implementing Security Policies and Procedures Researching and Analyzing Industry Trends Integrating Computing, Communications and Business Disciplines Additionally, you can download a suite of study tools to help you prepare including an assessment test, two practice exams, electronic flashcards, and a glossary of key terms. Go to www.sybex.com/go/casp and download the full set of electronic test prep tools.

Practical Aviation Security John Wiley & Sons

The threats of economic espionage and intellectual property (IP) theft are global, stealthy, insidious, and increasingly common. According to the U.S. Commerce Department, IP theft is estimated to top $250 billion annually and also costs the United States approximately 750,000 jobs. The International Chamber of Commerce puts the global fiscal loss at more than $600 billion a year. Secrets Stolen, Fortunes Lost offers both a fascinating journey into the underside of the Information Age, geopolitics, and global economy, shedding new light on corporate hacking, industrial espionage, counterfeiting and piracy, organized crime and related problems, and a comprehensive guide to developing a world-class defense against these threats. You will learn what you need to know about this dynamic global phenomenon (how it happens, what it costs, how to build an effective program to mitigate risk and how corporate culture determines your success), as well as how to deliver the message to the boardroom and the workforce as a whole. This book serves as an invaluable reservoir of ideas and energy to draw on as you develop a winning security strategy to overcome this formidable challenge. It’s Not “Someone Else’s Problem: Your Enterprise is at Risk Identify the dangers associated with intellectual property theft and economic espionage The Threat Comes from Many Sources Describes the types of attackers, threat vectors, and modes of attack The Threat is Real Explore case studies of real-world incidents in stark relief How to Defend Your Enterprise Identify all aspects of a comprehensive program to tackle such threats and risks How to Deliver the Message: Awareness and Education Adaptable content (awareness and education materials, policy language, briefing material, presentations, and assessment tools) that you can incorporate into your security program now

Information Security Governance Simplified Crabtree Publishing Company

Cyber-attacks are a real and increasing threat. Cybercrime industry is 24 x 7, where Cybercriminals are continuously advancing their skills with cutting edge tools and technology resources at their fingertips. While, technical courses and certifications are working on addressing the skills shortage, there is still lack of practical knowledge and awareness amongst the technology leaders about Cyber Risk Management. Most leaders have limited exposure to real life cyber-attack scenarios, if at all. This book takes technology leaders from cybersecurity theory to practical knowledge. It guides them on how to manage and mitigate cyber risks; implement and remediate cyber controls. In the event of a real-life cyber-attack, this book can be an invaluable guide for a technology leader who does not know where to begin and what questions to ask. It is not a matter of ‘if’, but ‘when..’ so use this book as a guide to start those critical discussions today, before it is too late.

Careers in School Safety Universal-Publishers

School security can be a pretty tough job, it is not just about patrolling halls and checking in students for the day. Students and faculty today face a lot of potential dangers, including cyberbullying, drug use, and violence. A school resource or security officer is tasked with keeping people safe, taking action when necessary, but also simply mentoring students and helping shape school policy. This comprehensive volume takes career seekers through the ups and downs of training to take on the important job of keeping schools safe. It offers some tips on interviews and resumes and includes real-life experience from those in the field.

Loss Control Auditing Butterworth-Heinemann

Many organizations encounter a common problem in their approach to intranet security: They treat intranets as an internal tool that is hidden deep in the corporate network and is somehow immune from external attacks. This is far from the truth, however. An intranet is basically a Web application exposed to a hostile environment the same way as the corporate Web site and therefore vulnerable to the same scope of threats. The fact that it is intended for employees and trusted parties doesn’t guarantee anything against hacker attacks, viruses, and spam. Failing to introduce a dedicated intranet security policy entails a range of risks associated with sensitive information leakage and data loss. For many organizations, safeguarding intranets is even more important than protecting their Web sites. Intranets usually contain extremely confidential assets crucial for both day-to-day activity and strategic business development. A successful attack may result in disruption of the organization’s operations, significant reputation damage, and infringement of legal regulations. To avoid unexpected embarrassment after launching an intranet, organizations must carefully evaluate the solution’s capability to cope with security issues. So, with the preceding in mind, this chapter provides information about all aspects of threats that affect intranet security. The chapter is intended for organizations that understand the changing nature of the threat landscape and what might be done to mitigate it.

Network and System Security Dan Sommer

A jargon-busting guide to the key concepts, terminology, and technologies of cybersecurity. Perfect for anyone planning or implementing a security strategy. In Making Sense of Cybersecurity you will learn how to: Develop and incrementally improve your own cybersecurity strategy Detect rogue WiFi networks and safely browse on public WiFi Protect against physical attacks utilizing USB devices or building access cards Use the OODA loop and a hacker mindset to plan out your own attacks Connect to and browse the Dark Web Apply threat models to build, measure, and improve your defenses Respond to a detected cyber attack and work through a security breach Go behind the headlines of famous attacks and learn lessons from real-world breaches that author Tom Kranz has personally helped to clean up. Making Sense of Cybersecurity is full of clear-headed advice and examples that will help you identify risks in your organization and choose the right path to apply the important security concepts. You'll learn the three pillars of a successful security strategy and how to create and apply threat models that will iteratively improve your organization's readiness. Foreword by Naz Markuta. About the technology Someone is attacking your business right now. Understanding the threats, weaknesses, and attacks gives you the power to make better decisions about how to secure your systems. This book guides you through the concepts and basic skills you need to make sense of cybersecurity. About the book Making Sense of Cybersecurity is a crystal-clear overview of common cyber threats written for business and technical readers with no background in security. You’ll explore the core ideas of cybersecurity so you can effectively talk shop, plan a security strategy, and spot your organization’s own weak points. By examining real-world security examples, you’ll learn how the bad guys think and how to handle live threats. What's inside Develop and improve your cybersecurity strategy Apply threat models to build, measure, and improve your defenses Detect rogue WiFi networks and safely browse on public WiFi Protect against physical attacks About the reader For anyone who needs to understand computer security. No IT or cybersecurity experience required. About the author Tom Kranz is a security consultant with over 30 years of experience in cybersecurity and IT. Table of Contents 1 Cybersecurity and hackers 2 Cybersecurity: Everyone’s problem PART 1 3 Understanding hackers 4 External attacks 5 Tricking our way in: Social engineerin 6 Internal attacks 7 The Dark Web: Where is stolen data traded? PART 2 8 Understanding risk 9 Testing your systems 10 Inside the security operations center 11 Protecting the people 12 After the hack

Secure Software Design Lulu.com

Key Strategies to Safeguard Your Future Well Aware offers a timely take on the leadership issues that businesses face when it comes to the threat of hacking. Finney argues that cybersecurity is not a technology problem; it’s a people problem. Cybersecurity should be understood as a series of nine habits that should be mastered—literacy, skepticism, vigilance, secrecy, culture, diligence, community, mirroring, and deception—drawn from knowledge the author has acquired during two decades of experience in cybersecurity. By implementing these habits and changing our behaviors, we can combat most security problems. This book examines our security challenges using lessons learned from psychology, neuroscience, history, and economics. Business leaders will learn to harness effective cybersecurity techniques in their businesses as well as their everyday lives.

SSCP (ISC)2 Systems Security Certified Practitioner Official Study Guide Jones & Bartlett Publishers

CompTIA Security+ Study Guide (Exam SY0-601)

Physical Security for IT CRC Press

Loss Control Auditing: A Guide for Conducting Fire, Safety, and Security Audits is a one-stop resource for both developing and executing a loss control audit program. This fully updated second edition addresses loss control auditing from the perspectives of workplace safety, physical security, and fire risks. It focuses on the three core areas of an audit: documentation review, physical inspection, and employee interviews, and presents a three-phase model – pre-audit, audit, and post-audit activities – which can be used for all three core areas. This new edition benefits from the addition of auditing and system measurement material as promulgated in ISO 45001 and ANSI/ASSP Z10 standards and the Occupational Safety and Health Administration’s Recommended Practices for Safety and Health Programs. It offers an expanded discussion of the application of auditing to the field of emergency management and new text explaining how leading and lagging measures can be used in the auditing process during assessment as well as in the post-audit evaluation. Subsidiary organizations and their integration into the auditing process, such as the areas of contractor management and temporary worker safety are covered in detail. The book discusses the integration of qualitative and quantitative measures in an effort to arrive at a more holistic scoring mechanism to assess organizational performance. In all, the depth of material presented in this thorough book showcases how to develop and execute a loss control management system audit program to a high quality. An ideal read for industry professionals, students, and postgraduates in the fields of fire service, loss prevention, and safety management.

Ensuring Information Assets Protection CRC Press

Uniting broad, time-tested security principles and the author’s 35-plus years of experience with international security, intelligence, and foreign affairs, Understanding Personal Security: A Guide for Business Travelers offers a detailed yet practical framework on which to develop personal security awareness and training programs. As a critical resource for any travelers who may need to make fast, smart judgements in high-risk environments, this book helps readers analyze threats, threat actors, and the common adversarial characteristics, as well as the function of risk as a differentiating principle. This versatile text blends abstract organizing principles with street honed instincts, becoming equally valuable to security managers with previous experience and those corporate or non-profit organizations with employees in developing nations.

Bodyguards Syngress

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

Cybersecurity for Executives Delmar

NOTE: The exam this book covered, CASP: CompTIA Advanced Security Practitioner (Exam CAS-002), was retired by CompTIA in 2019 and is no longer offered. For coverage of the current exam CASP+ CompTIA Advanced Security Practitioner: Exam CAS-003, Third Edition, please look for the latest edition of this guide: CASP+ CompTIA Advanced Security Practitioner Study Guide: Exam CAS-003, Third Edition (9781119477648). CASP: CompTIA Advanced Security Practitioner Study Guide: CAS-002 is the updated edition of the bestselling book covering the CASP certification exam. CompTIA approved, this guide covers all of the CASP exam objectives with clear, concise, thorough information on crucial security topics. With practical examples and insights drawn from real-world experience, the book is a comprehensive study resource with authoritative coverage of key concepts. Exam highlights, end-of-chapter reviews, and a searchable glossary help with information retention, and cutting-edge exam prep software offers electronic flashcards and hundreds of bonus practice questions. Additional hands-on lab exercises mimic the exam's focus on practical application, providing extra opportunities for readers to test their skills. CASP is a DoD 8570.1-recognized security certification that validates the skillset of advanced-level IT security professionals. The exam measures the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments, as well as the ability to think critically and apply good judgment across a broad spectrum of security disciplines. This study guide helps CASP candidates thoroughly prepare for the exam, providing the opportunity to: Master risk management and incident response Sharpen research and analysis skills Integrate computing with communications and business Review enterprise management and

technical component integration Experts predict a 45-fold increase in digital data by 2020, with one-third of all information passing through the cloud. Data has never been so vulnerable, and the demand for certified security professionals is increasing quickly. The CASP proves an IT professional's skills, but getting that certification requires thorough preparation. This CASP study guide provides the information and practice that eliminate surprises on exam day. Also available as a set, Security Practitoner & Crypotography Set, 9781119071549 with Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition.

Modern Operatives Elsevier

Fully updated Study Guide for the SSCP This guide prepares you for the SSCP, Systems Security Certified Practitioner certification examination by focusing on the Common Body of Knowledge (CBK) as determined by ISC2 in seven high level topics. This Sybex Study Guide covers 100% of all exam objectives. You'll prepare for the exam smarter and faster with Sybex thanks to expert content, real-world practice, access to the Sybex online interactive learning environment and much more. Reinforce what you've learned with key topic exam essentials and chapter review questions. Along with the book you also get access to Sybex's superior online interactive learning environment that includes: 125 question practice exam to help you identify where you need to study more. Get more than 90 percent of the answers correct, you're ready to take the certification exam. More than 100 Electronic Flashcards to reinforce your learning and give you last minute test prep before the exam A searchable glossary in PDF to give you instant access to the key terms you need to know for the exam Appendix of charts, tables, typical applications, and programs Coverage of all of the exam topics in the book means you'll be ready for: Access Controls Security Operations and Administration Risk Identification, Monitoring and Analysis Incident Response and Recovery Cryptography Network and Communications Security Systems and Application Security

CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide Springer Nature

Strategic Security will help security managers, and those aspiring to the position, to think strategically about their job, the culture of their workplace, and the nature of security planning and implementation. Security professionals tend to focus on the immediate (the urgent) rather than the important and essential—too often serving as "firefighters" rather than strategists. This book will help professionals consider their roles, and structure their tasks through a strategic approach without neglecting their career objectives. Few security management books for professionals in the field focus on corporate or industrial security from a strategic perspective. Books on the market normally provide "recipes," methods or guidelines to develop, plans, policies or procedures. However, many do so without taking into account the personal element that is supposed to apply these methods. In this book, the authors helps readers to consider their own career development in parallel with establishing their organisation security programme. This is fundamental to becoming, and serving as, a quality, effective manager. The element of considering career objectives as part-and-parcel to this is both unique to only this book and vital for long-term career success. The author delineates what makes strategic thinking different in a corporate and security environment. While strategy is crucial in the running of a company, the traditional attitude towards security is that it has to fix issues quickly and at low cost. This is an attitude that no other department would tolerate, but because of its image, security departments sometimes have major issues with buy-in and from top-management. The book covers the necessary level of strategic thinking to put their ideas into practice. Once this is achieved, the strategic process is explained, including the need to build the different steps into this process—and into the overarching business goals of the organisation—will be demonstrated. The book provides numerous hand-on examples of how to formulate and execute the strategic master plan for the organization. The authors draws on his extensive experience and successes to serve as a valuable resource to all security professionals looking to advance their careers in the field.

The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-601) The Rosen Publishing Group, Inc

Network and System Security provides focused coverage of network and system security technologies. It explores practical solutions to a wide range of network and systems security issues. Chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors’ respective areas of expertise. Coverage includes building a secure organization, cryptography, system intrusion, UNIX and Linux security, Internet security, intranet security, LAN security; wireless network security, cellular network security, RFID security, and more. Chapters contributed by leaders in the field covering foundational and practical aspects of system and network security, providing a new level of technical expertise not found elsewhere Comprehensive and updated coverage of the subject area 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

Building a Practical Information Security Program Morgan Kaufmann

The role of bodyguard or close protection officer" is highly misunderstood. In action films, threats are obvious: ski-mask wearing gunmen fire at the client from a speeding black Suburban truck. In real life, threats may be harder to assess. If a crowd of unarmed protesters blocks the client's access to his or her car as well as the building they are being escorted to, this poses a threat. However, bodyguards have no legal right to use force in a public place unless they are being attacked. Usually bodyguards are the ones who call the police. This interesting new book examines the different types of bodyguard - police, military and civilian; their training; typical roles; the equipment they use; weapons; bodyguards and the law; evasive driving; and life as a bodyguard.

CASP CompTIA Advanced Security Practitioner Study Guide Lulu.com

The physical security of IT, network, and telecommunications assets is equally as important as cyber security. We justifiably fear the hacker, the virus writer and the cyber terrorist. But the disgruntled employee, the thief, the vandal, the corporate foe, and yes, the terrorist can easily cripple an organization by doing physical damage to IT assets. In many cases such damage can be far more difficult to recover from than a hack attack or malicious code incident. It does little good to have great computer security if wiring closets are easily accessible or individuals can readily walk into an office and sit down at a computer and gain access to systems and applications. Even though the skill level required to hack systems and write viruses is becoming widespread, the skill required to wield an ax, hammer, or fire hose and do thousands of dollars in damage is even more common. Although many books cover computer security from one perspective or another, they do not thoroughly address physical security. This book shows organizations how to design and implement physical security plans. It provides practical, easy-to-understand and readily usable advice to help organizations to improve physical security for IT, network, and telecommunications assets. * Expert advice on identifying physical security needs * Guidance on how to design and implement security plans to prevent the physical destruction of, or tampering with computers, network equipment, and telecommunications systems * Explanation of the processes for establishing a physical IT security function * Step-by-step instructions on how to accomplish physical security objectives * Illustrations of the major elements of a physical IT security plan * Specific guidance on how to develop and document physical security methods and procedures

Making Sense of Cybersecurity John Wiley & Sons

This Bodyguard / Executive Protection Specialist Career Preparation & Instructional Training Guide was developed to provide useful information that will support the preparation process when assigned to protecting Life and Property. Although every scenario and situation you may encounter is different, this training guide will assist you on the development of your own preparation and career goals when entering the Security Industry.