Corporate Computer Security 4th Edition

This is the most comprehensive book on computer security on themarket, with 23 chapters and 29 Appendices covering virtually allaspects of computer security. Chapters are contributed by recognized experts in theindustry. This title has come to be known as "Big Blue" in industrycircles and has a reputation for being the reference for computersecurity issues.

This is the must-have book for a must-know field. Today, general security knowledge is mandatory, and, if you who need to understand the fundamentals, Computer Security Basics 2nd Edition is the book to consult. The new edition builds on the well-established principles developed in the original edition and thoroughly updates that core knowledge. For anyone involved with computer security, including security administrators, system administrators, developers, and IT managers, Computer Security Basics 2nd Edition offers a clear overview of the security concepts you need to know, including access controls, malicious software, security policy, cryptography, biometrics, as well as government regulations and standards. This handbook describes complicated concepts such as trusted systems, encryption, and mandatory access control in simple terms. It tells you what you need to know to understand the basics of computer security, and it will help you persuade your employees to practice safe computing. Topics include: Computer security concepts Security breaches, such as viruses and other malicious programs Access controls Security policy Web attacks Communications and network security Encryption Physical security and biometrics Wireless network security Computer security and requirements of the Orange Book OSI Model and TEMPEST

Marcus, alias w1n5t0n, is slim, snel en wired met het netwerk. Het kost hem geen moeite de bewakingssystemen van zijn middelbare school te omzeilen. Zijn wereld wordt echter op zijn kop gezet als hij en zijn vrienden te maken krijgen met de naschokken van een grote terreuraanslag. Ze zijn op het verkeerde moment op de verkeerde plek, en worden gearresteerd, opgesloten en meedogenloos ondervraagd door Homeland Security. Wanneer hij eindelijk vrijkomt, ontdekt Marcus dat zijn stad een politiestaat is geworden, waar elke burger wordt behandeld als een potentiële terrorist. Niemand gelooft wat hem en zijn vrienden is overkomen, en dus heeft hij maar een uitweg: zelf Homeland Security aanpakken. Cory Doctorow (1971) is co-editor van Boing Boing een van de populairste blogs ter wereld. Hij won diverse prijzen, waaronder de Nebula en de Campbell Award en wordt gezien als een Young Global Leader van het web.

For introductory courses in IT Security. A strong business focus through a solid technical presentation of security tools. Corporate Computer Security provides a strong business focus along with a solid technical understanding of security tools. This text gives students the IT security skills they need for the workplace. This edition is more business focused and contains additional hands-on projects, coverage of wireless and data security, and case studies. This program will provide a better teaching and learning experience-for you and your students. Here's how: Encourage Student's to Apply Concepts: Each chapter now contains new hands-on projects that use contemporary software. Business Environment Focus: This edition includes more of a focus on the business applications of the concepts. Emphasis has been placed on securing corporate information systems, rather than just hosts in general. Keep Your Course Current and Relevant: New examples, exercises, and research findings appear throughout the text.

This book discusses the implementation of privacy by design in Europe, a principle that has been codified within the European Data Protection Regulation (GDPR). While privacy by design inspires hope for future privacy-sensitive designs, it also introduces the need for a common understanding of the legal and technical concepts of privacy and data protection. By pursuing an interdisciplinary approach and comparing the problem definitions and objectives of both disciplines, this book bridges the gap between the legal and technical fields in order to enhance the regulatory and academic discourse. The research presented reveals the scope of legal principles and technical tools for privacy protection, and shows that the concept of privacy by design goes beyond the principle of the GDPR. The book presents an analysis of how current regulations delegate the implementation of technical privacy and data protection measures to developers and describes how policy design must evolve in order to implement privacy by design and default principles.

Held October 13-16, 1992. Emphasizes information systems security criteria (& how it affects us), and the actions associated with organizational accreditation. These areas are highlighted by emphasizing how organizations are integrating information security solutions. Includes presentations from government, industry and academia and how they are cooperating to extend the state-of-the-art technology to information systems security. 72 referred papers, trusted systems tutorial and 23 executive summaries. Very valuable! Must buy!

Whether you are active in security management or studying for the CISSP exam, you need accurate information you can trust. A practical reference and study guide, Information Security Management Handbook, Fourth Edition, Volume 3 prepares you not only for the CISSP exam, but also for your work as a professional. From cover to cover the book gives you the information you need to understand the exam's core subjects. Providing an overview of the information security arena, each chapter presents a wealth of technical detail. The changes in the technology of information security and the increasing threats to security from open systems make a complete and up-to-date understanding of this material essential. Volume 3 supplements the information in the earlier volumes of this handbook, updating it and keeping it current. There is no duplication of material between any of the three volumes. Because the knowledge required to master information security - the Common Body of Knowledge (CBK) - is growing so quickly, it requires frequent updates. As a study guide or resource that you can use on the job, Information Security Management Handbook, Fourth Edition, Volume 3 is the book you will refer to over and over again.

For introductory courses in IT Security. A strong business focus through a solid technical presentation of security tools. Corporate Computer Security provides a strong business focus along with a solid technical understanding of security tools. This text gives students the IT security skills they need for the workplace. This edition is more business focused and contains additional hands-on projects, coverage of wireless and data security, and case studies. This program will provide a better teaching and learning experience-for you and your students. Here's how: *Encourage Student's to Apply Concepts: Each chapter now contains new hands-on projects that use contemporary software. *Business Environment Focus: This edition includes more of a focus on the business applications of the concepts. Emphasis has been placed on securing corporate information systems, rather than just hosts in general. *Keep Your Course Current and Relevant: New examples, exercises, and research findings appear throughout the text.

This interdisciplinary collection places corporate security in a theoretical and international context. Arguing that corporate security is becoming the primary form of security in the twenty-first century, it explores a range of issues including regulation, accountability, militarization, strategies of securitization and practitioner techniques.

The Regulation of Corporate Disclosure is a one-volume treatise on the disclosure regime in place under the Federal securities laws. The treatise addresses the formal disclosure process (periodic reports, MD&A, Regulation FD), the informal disclosure process (press releases, social media, discussions with analysts), and the application of the antifraud provisions to these communications. The treatise includes chapters on scienter and materiality, and also addresses communications with and disclosure obligations to shareholders. The Fourth Edition has been significantly revised and, among other topics, includes coverage of: The duties and responsibilities of corporate officials relating to the disclosure process The most recent cases addressing disclosure issues, including decisions by the Supreme Court on topics such as the application of the antifraud provisions to beliefs and opinions Pronouncements by the U.S. Securities and Exchange Commission on disclosure issues, including consideration of the SEC's efforts to improve disclosure effectiveness The developing need to consider disclosure of public interest matters, including the effects of climate change on a company's business The disclosure requirements applicable to the proxy process, including the system for uncovering the identity of street name owners State disclosure obligations of the board of directors under its fiduciary obligations to shareholders.

Business Legislation for Management is meant for students of business management, who need to be familiar with business laws and company law in their future role as managers. The book explains these laws in a simple and succinct manner, making the students sufficiently aware of the scope of these laws so that they are able to operate their businesses within their legal confines. The book approaches the subject in a logical way, so that even a student with no legal background is able to understand it. The book is the outcome of the authors' long experience of teaching business law and company law to students pursuing undergraduate and postgraduate courses at the University of Delhi. This, in fact, has made it possible for them to write on law without the use of legal jargon; thus ensuring that even the most complicated provisions of various legislations are explained in an easily comprehensible manner. This new edition of the book has been thoroughly updated, revised and expanded keeping in mind the requirements of diverse syllabuses of various universities. New in this Edition • Laws of Intellectual Property Rights that include Patents Act, 1970, Copyright Act, 1957, Trade Marks Act, 1999, and Designs Act, 2000 • Foreign Exchange Management Act, 1999 • Competition Act, 2002 Salient Features • Unfolds intricate points of law to solve intriguing questions • Elucidates practical implications of law through a large number of illustrations

This is the eBook of the printed book and may not include any media, website access codes, or print supplements that may come packaged with the bound book. For introductory courses in IT Security. A strong business focus through a solid technical presentation of security tools. Corporate Computer Security provides a strong business focus along with a solid technical understanding of security tools. This text gives students the IT security skills they need for the workplace. This edition is more business focused and contains additional hands-on projects, coverage of wireless and data security, and case studies. This program will provide a better teaching and learning experience–for you and your students. Here’s how: Encourage Student’s to Apply Concepts: Each chapter now contains new hands-on projects that use contemporary software. Business Environment Focus: This edition includes more of a focus on the business applications of the concepts. Emphasis has been placed on securing corporate information systems, rather than just hosts in general. Keep Your Course Current and Relevant: New examples, exercises, and research findings appear throughout the text.

The new edition of a bestseller, Information Technology Control and Audit, Fourth Edition provides a comprehensive and up-to-date overview of IT governance, controls, auditing applications, systems development, and operations. Aligned to and supporting the Control Objectives for Information and Related Technology (COBIT), it examines emerging trend

The book has been written for 'Business Laws' Paper of the MBA Programme, Semester-II examination of the Gautam Buddh Technical University in accordance with its new syllabus, effective from the academic year 2013-14. Its contents have been largely extracted from the author's reputed title 'Business Legislation for Management' which has gained tremendous readership over the years. This book presents the subject matter tailor-made, as per the revised course structure of the Paper, to enable the students to possess a textbook which caters to their needs in full. The book has been organized into six units, namely, Law of Contract, Law of Partnership and Law of Sale of Goods, Law of Negotiable Instruments, Company Law and Law of Consumer Protection, Law of Information Technology, and Law of Right to Information. Key Features • Quotes Indian and English cases at appropriate places with a view to ensure necessary authenticity and clarity on the subject. • Includes text questions and practical problems with hints and solutions in each chapter to enable students to evaluate their understanding of the subject • Explains complicated provisions in easily comprehensible language with the help of illustrations and analogies

Principles of Information Security
Databases
Computer Security Handbook, Set
Business Laws (For GBTU), 4th Edition
Emerging Organizational, Ethical, and Human Issues
Corporate Computer Security
Business Legislation for Management, 4th Edition
Computer Security Basics
Encyclopedia of Information Science and Technology, Fourth Edition
Principles of Computer Security Lab Manual, Fourth Edition

Security Operations Management takes concepts from business administration and criminal justice schools and incorporates them into the world of security management. It is comprehensive text focused on theoretical and research-oriented overviews of the core principles of security

management. The book includes critical issues faced by real-life security practitioners and explores how they were resolved. The book is written for practitioners, students, and general managers who wish to understand and manage security operations more effectively. The book explains the difficult task of bringing order to the security department's responsibilities of protecting people, intellectual property, physical assets and opportunity. In addition, the book covers theoretical and practical management-oriented developments in the security field, including new business models and e-management strategies. Discussions provide coverage of both the business and technical sides of security. Numerous case histories illustrating both the business and technical sides of security. Strategies for outsourcing security services and systems.

Written by leading information security educators, this fully revised, full-color computer security textbook covers CompTIA’s fastest-growing credential, CompTIA Security+. Principles of Computer Security, Fourth Edition is a student-tested, introductory computer security textbook that provides comprehensive coverage of computer and network security fundamentals in an engaging and dynamic full-color design. In addition to teaching key computer security concepts, the textbook also fully prepares you for CompTIA Security+ exam SY0-401 with 100% coverage of all exam objectives. Each chapter begins with a list of topics to be covered and features sidebar exam and tech tips, a chapter summary, and an end-of-chapter assessment section that includes key term, multiple choice, and essay quizzes as well as lab projects. Electronic content includes CompTIA Security+ practice exam questions and a PDF copy of the book. Key features: CompTIA Approved Quality Content (CAQC) Electronic content features two simulated practice exams in the Total Tester exam engine and a PDF eBook Supplemented by Principles of Computer Security Lab Manual, Fourth Edition, available separately White and Conklin are two of the most well-respected computer security educators in higher education Instructor resource materials for adopting instructors include: Instructor Manual, PowerPoint slides featuring artwork from the book, and a test bank of questions for use as quizzes or exams Answers to the end of chapter sections are not included in the book and are only available to adopting instructors Learn how to: Ensure operational, organizational, and physical security Use cryptography and public key infrastructures (PKIs) Secure remote access, wireless networks, and virtual private networks (VPNs) Authenticate users and lock down mobile devices Harden network devices, operating systems, and applications Prevent network attacks, such as denial of service, spoofing, hijacking, and password guessing Combat viruses, worms, Trojan horses, and rootkits Manage e-mail, instant messaging, and web security Explore secure software development requirements Implement disaster recovery and business continuity measures Handle computer forensics and incident response Understand legal, ethical, and privacy issues

Called "the leader in the Snort IDS book arms race" by Richard Bejtlich, top Amazon reviewer, this brand-new edition of the best-selling Snort book covers all the latest features of a major upgrade to the product and includes a bonus DVD with Snort 2.1 and other utilities. Written by the same lead engineers of the Snort Development team, this will be the first book available on the major upgrade from Snort 2 to Snort 2.1 (in this community, major upgrades are noted by .x and not by full number upgrades as in 2.0 to 3.0). Readers will be given invaluable insight into the code base of Snort, and in depth tutorials of complex installation, configuration, and troubleshooting scenarios. Snort has three primary uses: as a straight packet sniffer, a packet logger, or as a full-blown network intrusion detection system. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes. Snort uses a flexible rules language to describe traffic that it should collect or pass, a detection engine that utilizes a modular plug-in architecture, and a real-time alerting capability. A CD containing the latest version of Snort as well as other up-to-date Open Source security utilities will accompany the book. Snort is a powerful Network Intrusion Detection System that can provide enterprise wide sensors to protect your computer assets from both internal and external attack. * Completly updated and comprehensive coverage of snort 2.1 * Includes free CD with all the latest popular plug-ins * Provides step-by-step instruction for installing, configuring and troubleshooting

The growing complexity of today's interconnected systems has not only increased the need for improved information security, but also helped to move information from the IT backroom to the executive boardroom as a strategic asset. And, just like the tip of an iceberg is all you see until you run into it, the risks to your information are mostly invi

Achieve the gold standard in penetration testing with Kali using this masterpiece, now in its fourth edition Key Features Rely on the most updated version of Kali to formulate your pentesting strategies Test your corporate network against threats Explore new cutting-edge wireless penetration tools and features Book Description Kali Linux is a comprehensive penetration testing platform with advanced tools to identify, detect, and exploit the vulnerabilities uncovered in the target network environment. With Kali Linux, you can apply the appropriate testing methodology with defined business objectives and a scheduled test plan, resulting in successful penetration testing project engagement. This fourth edition of Kali Linux 2018: Assuring Security by Penetration Testing starts with the installation of Kali Linux. You will be able to create a full test environment to safely practice scanning, vulnerability assessment, and exploitation. You'll explore the essentials of penetration testing by collecting

relevant data on the target network with the use of several footprinting and discovery tools. As you make your way through the chapters, you'll focus on specific hosts and services via scanning and run vulnerability scans to discover various risks and threats within the target, which can then be exploited. In the concluding chapters, you'll apply techniques to exploit target systems in order to gain access and find a way to maintain that access. You'll also discover techniques and tools for assessing and attacking devices that are not physically connected to the network, including wireless networks. By the end of this book, you will be able to use NetHunter, the mobile version of Kali Linux, and write a detailed report based on your findings. What you will learn Conduct the initial stages of a penetration test and understand its scope Perform reconnaissance and enumeration of target networks Obtain and crack passwords Use Kali Linux NetHunter to conduct wireless penetration testing Create proper penetration testing reports Understand the PCI-DSS framework and tools used to carry out segmentation scans and penetration testing Carry out wireless auditing assessments and penetration testing Understand how a social engineering attack such as phishing works Who this book is for This fourth edition of Kali Linux 2018: Assuring Security by Penetration Testing is for pentesters, ethical hackers, and IT security professionals with basic knowledge of Unix/Linux operating systems. Prior knowledge of information security will help you understand the concepts in this book

Een van de grootste problemen van de economie is de opeenhoping en de verdeling van kapitaal. Dat hangt nauw samen met problemen van ongelijkheid, van concentratie van welvaart en van economische groei. Bevredigende oplossingen voor die problemen waren tot nu toe moeilijk te vinden. Theorieën te over, maar relevant historisch onderzoek was niet voorhanden. In Kapitaal in de 21ste eeuw analyseert Thomas Piketty een groot aantal gegevens uit de laatste twee eeuwen en uit twintig landen. Zo weet hij fundamentele economische en sociale processen bloot te leggen. Hij toont aan dat de moderne economische groei en de spreiding van kennis ons in staat hebben gesteld om de ongelijkheid op apocalyptische schaal die Marx had voorspeld te voorkomen. Maar de diepere structuur van kapitaal en ongelijkheid is er in wezen niet door veranderd, zoals we in ons optimisme na de Tweede Wereldoorlog dachten. De belangrijkste oorzaak van de ongelijkheid is de tendens dat de opbrengst op kapitaal groter is dan de economische groei - iets wat nu tot extreme ongelijkheid dreigt te leiden. Het wakkert de onvrede aan en ondermijnt democratische verworvenheden. Het is aan de politiek om die tendens in te tomen. Kapitaal in de 21ste eeuw is een buitengewoon ambitieuze onderneming, waarvan de grote waarde alom wordt erkend. Het is een herbezinning op de economische geschiedenis en het dwingt ons de werkelijkheid nuchter onder ogen te zien.

Over 10,000 Detailed Entries! "There is a myth that all stakeholders in the healthcare space understand the meaning of basic information technology jargon. In truth, the vernacular of contemporary medical information systems is unique, and often misused or misunderstoodÖ Moreover, an emerging national Heath Information Technology (HIT) architecture; in the guise of terms, definitions, acronyms, abbreviations and standards; often puts the non-expert medical, nursing, public policy administrator or paraprofessional in a position of maximum uncertainty and minimum productivity ÖThe Dictionary of Health Information Technology and Security will therefore help define, clarify and explain...You will refer to it daily." -- Richard J. Mata, MD, MS, MS-CIS, Certified Medical Planner© (Hon), Chief Medical Information Officer [CMIO], Ricktelmed Information Systems, Assistant Professor Texas State University, San Marcos, Texas An Essential Tool for Every Health Care Industry Sector: layman, purchaser, and benefits manager physician, provider and healthcare facility payer, intermediary and consulting professional Key Benefits & Features Include: New HIT, HIPAA, WHCQA, HITPA, and NEPSI terminology Abbreviations, acronyms, and slang-terms defined Illustrations and simple examples Cross-references to current research

Information Technology Control and Audit
Computer Security Journal
Principles of Computer Security, Fourth Edition
Dictionary of Health Information Technology and Security
Kali Linux 2018
Official (ISC)2 Guide to the CISSP CBK - Fourth Edition
Security Operations Management
Data Protection by Design and Default for the Internet of Things
Computer Security
Theory and Practice in International Perspective

Practice the Computer Security Skills You Need to Succeed! 40+ lab exercises challenge you to solve problems based on realistic case studies Step-by-step scenarios require you to think critically Lab analysis tests measure your understanding of lab results Key term quizzes help build your vocabulary Labs can be performed on a Windows, Linux, or Mac platform with the use of virtual machines In this Lab Manual, you'll practice Configuring workstation network connectivity Analyzing network communication Establishing secure network application communication using TCP/IP protocols Penetration testing with Nmap, metasploit, password cracking, Cobalt Strike, and other tools Defending against network application attacks, including SQL injection, web browser exploits, and email attacks Combatting Trojans, man-in-the-middle attacks, and steganography Hardening a host computer, using antivirus applications, and

configuring firewalls Securing network communications with encryption, secure shell (SSH), secure copy (SCP), certificates, SSL, and IPsec Preparing for and detecting attacks Backing up and restoring data Handling digital forensics and incident response Instructor resources available: This lab manual supplements the textbook Principles of Computer Security, Fourth Edition, which is available separately Virtual machine files Solutions to the labs are not included in the book and are only available to adopting instructors

In recent years, our world has experienced a profound shift and progression in available computing and knowledge sharing innovations. These emerging advancements have developed at a rapid pace, disseminating into and affecting numerous aspects of contemporary society. This has created a pivotal need for an innovative compendium encompassing the latest trends, concepts, and issues surrounding this relevant discipline area. During the past 15 years, the Encyclopedia of Information Science and Technology has become recognized as one of the landmark sources of the latest knowledge and discoveries in this discipline. The Encyclopedia of Information Science and Technology, Fourth Edition is a 10-volume set which includes 705 original and previously unpublished research articles covering a full range of perspectives, applications, and techniques contributed by thousands of experts and researchers from around the globe. This authoritative encyclopedia is an all-encompassing, well-established reference source that is ideally designed to disseminate the most forward-thinking and diverse research findings. With critical perspectives on the impact of information science management and new technologies in modern settings, including but not limited to computer science, education, healthcare, government, engineering, business, and natural and physical sciences, it is a pivotal and relevant source of knowledge that will benefit every professional within the field of information science and technology and is an invaluable addition to every academic and corporate library.

As an information security professional, it is essential to stay current on the latest advances in technology and the effluence of security threats. Candidates for the CISSP® certification need to demonstrate a thorough understanding of the eight domains of the CISSP Common Body of Knowledge (CBK®), along with the ability to apply this indepth knowledge to daily practices. Recognized as one of the best tools available for security professionals, specifically for the candidate who is striving to become a CISSP, the Official (ISC)²® Guide to the CISSP® CBK®, Fourth Edition is both up-to-date and relevant. Reflecting the significant changes in the CISSP CBK, this book provides a comprehensive guide to the eight domains. Numerous illustrated examples and practical exercises are included in this book to demonstrate concepts and real-life scenarios. Endorsed by (ISC)² and compiled and reviewed by CISSPs and industry luminaries around the world, this textbook provides unrivaled preparation for the certification exam and is a reference that will serve you well into your career. Earning your CISSP is a respected achievement that validates your knowledge, skills, and experience in building and managing the security posture of your organization and provides you with membership to an elite network of professionals worldwide.

The fourth edition of Principles of Information Security explores the field of information security and assurance with updated content including new innovations in technology and methodologies. Students will revel in the comprehensive coverage that includes a historical overview of information security, discussions on risk management and security technology, current certification information, and more. The text builds on internationally-recognized standards and bodies of knowledge to provide the knowledge and skills students need for their future roles as business decision-makers. Information security in the modern organization is a management issue which technology alone cannot answer; it is a problem that has important economic consequences for which management will be held accountable. Students can feel confident that they are using a standards-based, content-driven resource to prepare for their work in the field. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The runaway growth of computer viruses and worms and the ongoing nuisance posed by malicious hackers and employees who exploit the security vulnerabilities of open network protocols make the tightness of an organization's security system an issue of prime importance. And information systems technology is advancing at a frenetic pace. Against this background, the challenges facing information security professionals are increasing rapidly. Information Security Management Handbook, Fourth Edition, Volume 2 is an essential reference for anyone involved in the security of information systems.

Guarding Your Business outlines the organizational elements that must be in place to protect the information and physical assets of typical businesses and organizations. The book recognizes the need for an architecture integrated within the organizational environment for systematic protection. Such an architecture is offered along with the building blocks to make organizations resistant to human error and resilient under physical attack or natural disaster. The book addresses risk assessment, determination of quality-of-service levels that balance safety versus cost, security versus privacy, determination of access rights to data and software, and a security-conscious culture in the organization. Questions answered by experts from academia and industry include: How can one organize for security? What organizational structures, policies, and procedures must be in place? What legal and privacy issues must be addressed?

The classic and authoritative reference in the field of computer security, now completely updated and revised With the continued presence of large-scale computers; the proliferation of desktop, laptop, and handheld computers; and the vast international networks that interconnect them, the nature and extent of threats to computer security have grown enormously. Now in its fifth edition, Computer Security Handbook continues to provide authoritative guidance to identify and to eliminate these threats where possible, as well as to lessen any losses attributable to them. With seventy-seven chapters contributed by a panel of renowned industry professionals, the new edition has increased coverage in both breadth and depth of all ten domains of the Common Body of Knowledge defined by the International Information Systems Security Certification Consortium (ISC). Of the seventy-seven chapters in the fifth edition, twenty-five chapters are completely new, including: 1. Hardware Elements of Security 2. Fundamentals of Cryptography and Steganography 3. Mathematical models of information security 4. Insider threats 5. Social engineering and low-tech attacks 6. Spam, phishing, and Trojans: attacks meant to fool 7. Biometric authentication 8. VPNs and secure remote access 9. Securing Peer2Peer, IM, SMS, and collaboration tools 10. U.S. legal and regulatory security issues, such as GLBA and SOX Whether you are in charge of many computers or just one important one, there are immediate steps you can take to safeguard your computer system and its contents. Computer Security Handbook, Fifth Edition equips you to protect the information and networks that are vital to your organization.

We live in a wired society, with computers containing and passing around vital information on both personal and public matters. Keeping this data safe is of paramount concern to all. Yet, not a day seems able to pass without some new threat to our computers. Unfortunately, the march of technology has given us the benefits of computers and electronic tools, while also opening us to unforeseen dangers. Identity theft, electronic spying, and the like are now standard worries. In the effort to defend both personal privacy and crucial databases, computer security has become a key industry. A vast array of companies devoted to defending computers from hackers and viruses have cropped up. Research and academic institutions devote a considerable amount of time and effort to the study of information systems and computer security. Anyone with access to a computer needs to be aware of the developing trends and growth of computer security. To that end, this book presents a comprehensive and carefully selected bibliography of the literature most relevant to understanding computer security. Following the bibliography section, continued access is provided via author, title, and subject indexes. With such a format, this book serves as an important guide and reference tool in the defence of our computerised culture.

Law of the Internet, Fourth Edition is a two-volume up-to-date legal resource covering electronic commerce and online contracts, privacy and network security, intellectual property and online content management, secure electronic transactions, cryptography, and digital signatures, protecting intellectual property online through link licenses, frame control and other methods, online financial services and securities transactions, antitrust and other liability. The Law of the Internet, Fourth Edition quickly and easily gives you everything you need to provide expert counsel on: Privacy laws and the Internet Ensuring secure electronic transactions, cryptography, and digital signatures Protecting intellectual property online - patents, trademarks, and copyright Electronic commerce and contracting Online financial services and electronic payments Antitrust issues, including pricing, bundling and tying Internal network security Taxation of electronic commerce Jurisdiction in Cyberspace Defamation and the Internet Obscene and indecent materials on the Internet Regulation of Internet access and interoperability The authors George B. Delta and Jeffrey H. Matsuura -- two Internet legal experts who advise America's top high-tech companies -- demonstrate exactly how courts, legislators and treaties expand traditional law into the new context of the Internet and its commercial applications, with all the citations you'll need. The Law of the Internet also brings you up to date on all of the recent legal, commercial, and technical issues surrounding the Internet and provides you with the knowledge to thrive in the digital marketplace. Special features of this two-volume resource include timesaving checklists and references to online resources.

The new edition of a bestseller, Information Technology Control and Audit, Fourth Edition provides a comprehensive and up-to-date overview of IT governance, controls, auditing applications, systems development, and operations. Aligned to and supporting the Control Objectives for Information and Related Technology (COBIT), it examines emerging trends and defines recent advances in technology that impact IT controls and audits—including cloud computing, web-based applications, and server virtualization. Filled with exercises, review questions, section summaries, and references for further reading, this updated and revised edition promotes the mastery of the concepts and practical implementation of controls needed to manage information technology resources effectively well into the future. Illustrating the complete IT audit process, the text: Considers the legal environment and its impact on the IT field—including IT crime issues and protection against fraud Explains how to determine risk management objectives Covers IT project management and describes the auditor’s role in the process Examines advanced topics such as virtual infrastructure security, enterprise resource planning, web application risks and controls, and cloud and mobile computing security Includes review questions, multiple-choice questions with answers, exercises, and resources for further reading in each chapter This resource-rich text includes appendices with IT audit cases, professional standards, sample audit programs, bibliography of selected publications for IT auditors, and a glossary. It also considers IT auditor career development and planning and explains how to establish a career development plan. Mapping the requirements for information systems auditor

certification, this text is an ideal resource for those preparing for the Certified Information Systems Auditor (CISA) and Certified in the Governance of Enterprise IT (CGEIT) exams. Instructor's guide and PowerPoint® slides available upon qualified course adoption.

"This book provides a thorough understanding of issues and concerns in information technology security"--Provided by publisher.

The fast and easy way to get a job in Information Security Do you want to equip yourself with the knowledge necessary to succeed in the Information Security job market? If so, you've come to the right place. Packed with the latest and most effective strategies for landing a lucrative job in this popular and quickly-growing field, Getting an Information Security Job For Dummies provides no-nonsense guidance on everything you need to get ahead of the competition and launch yourself into your dream job as an Information Security (IS) guru. Inside, you'll discover the fascinating history, projected future, and current applications/issues in the IS field. Next, you'll get up to speed on the general educational concepts you'll be exposed to while earning your analyst certification and the technical requirements for obtaining an IS position. Finally, learn how to set yourself up for job hunting success with trusted and supportive guidance on creating a winning resume, gaining attention with your cover letter, following up after an initial interview, and much more. Covers the certifications needed for various jobs in the Information Security field Offers guidance on writing an attention-getting resume Provides access to helpful videos, along with other online bonus materials Offers advice on branding yourself and securing your future in Information Security If you're a student, recent graduate, or professional looking to break into the field of Information Security, this hands-on, friendly guide has you covered.

Enterprise Resource Planning (ERP) by Alexis Leon – In print for over two decades, continues to be a one-stop reference on the subject covering Basic Concepts, Benefits and Risks, ERP Related Technology, ERP Implementation Process, ERP Deployment Models, ERP Operations and Management, E-Business in ERP, and Future Directions in ERP. It is developed to be used as a conceptual resource for the students pursuing Management and Computer Science courses; and as a reference for the ERP Professionals. This book also examines enterprise software and shows the readers how ERP software can refine the operations of a company, how it can streamline its various overlapping functions, and how the core areas of any ERP package are related to each other. This fourth edition is substantially revised to keep pace with advances in ERP to provide a thorough introduction to the world of ERP and prepare the readers for a concrete understanding of today's ERP marketplace. Highlights: • Content presentation supports outcomes-based learning approach • 12 case studies on ERP software included, like: ◆SAP at Coca Cola Hellenic Bottling ◆3i Infotech at Faber-Castell India ◆Epicor at Knightsbridge Chemicals ◆Epicor at Howe Corporation ◆Ramco at Adani Logistics Ltd. ◆IQMS at Custom Profile ◆Sage at Agarwal Fasteners Pvt. Ltd. ◆Oracle JD Edwards at AVO Carbon India • Inclusion of contemporary topics like Business Intelligence, Business Analytics, e-Commerce, m-Commerce, Data Warehousing, Data Mining, SaaS and Cloud ERP with their Market Dynamics • Coverage on ERP Software like SAP, Infor, Epicor, QAD, 3i Infotech, Sage, Oracle etc. • Inclusion of functional features of SAP – Sales and Distribution, Controlling, Financial Integration, HCM, Production Planning, Quality Management. • Extensive pedagogical aid at the end of each chapter is provided.

Little brother
Een "Top-Down"-Benadering
De data-economie
Computer Security Handbook
National Computer Security Conference Proceedings, 1992
Guarding Your Business
Waarom data geld gaat vervangen, wat dit betekent voor onze economie en hoe je hierop in kunt spelen
Information Technology Control and Audit, Fourth Edition
Information Security Management Handbook, Fourth Edition