Legal Issues In Information Security Grama

When somebody should go to the ebook stores, search inauguration by shop, shelf by shelf, it is in point of fact problematic. This is why we allow the ebook compilations in this website. It will totally ease you to see guide **legal issues in information security grama** as you such as.

By searching the title, publisher, or authors of guide you really want, you can discover them rapidly. In the house, workplace, or perhaps in your method can be every best area within net connections. If you point toward to download and install the legal issues in information security grama, it is totally simple then, since currently we extend the join to purchase and make bargains to download and install legal issues in information security grama in view of that simple!

-

Legal and Privacy Issues in Information Security - Joanna Lyn Grama 2020-12-01 Thoroughly revised and updated to address the many changes in this evolving field, the third edition of Legal and Privacy Issues in Information Security addresses the complex relationship between the law and the practice of information security. Information systems security and legal compliance are 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 third 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

Designing Personalized User Experiences in eCommerce - Clare-Marie Karat 2006-04-11

How do you design personalized user experiences that delight and provide value to the customers of an eCommerce site? Personalization does not guarantee high quality user experience: a personalized user experience has the best chance of success if it is developed using a set of best practices in HCI. In this book 35 experts from academia, industry and government focus on issues in the design of personalized web sites. The topics range from the design and evaluation of user interfaces and tools to information architecture and computer programming related to commercial web sites. The book covers four main areas: -Theoretical, Conceptual, and Architectural Frameworks of Personalization, -Research on the Design and Evaluation of Personalized User Experiences in Different Domains, -Approaches to personalization Through Recommender Systems, -Lessons Learned and Future Research Questions. This book will be a valuable tool in helping the reader to understand the range of factors to take into consideration in designing and building a personalized user experience. The authors of each of the chapters identify possibilities and alert the reader to issues that can be addressed in the beginning of a project by taking a 'big picture' view of designing personalized user interfaces. For anyone working or studying in the field of HCI, information architecture or eCommerce, this book will provide a solid foundation of knowledge and prepare for the challenges ahead.

Internet Fraud Casebook - Joseph T. Wells 2010-07-26

Real case studies on Internet fraud written by real fraud examiners Internet Fraud Casebook: The World Wide Web of Deceit is a one-of-a-kind collection of actual cases written by the fraud examiners who investigated them. These stories were hand-selected from hundreds of submissions and together form a comprehensive, enlightening and entertaining picture of the many types of Internet fraud in varied industries throughout the world. Each case outlines how the fraud was engineered, how it was investigated, and how perpetrators were brought to justice Topics included are phishing, on-line auction fraud, security breaches, counterfeiting, and others Other titles by Wells: Fraud Casebook, Principles of Fraud Examination, and Computer Fraud Casebook This book reveals the dangers of Internet fraud and the measures that can be taken to prevent it from happening in the first place.

Cyberwarfare: Information Operations in a Connected World - Mike Chapple 2021-10-01

Cyberwarfare: Information Operations in a Connected World puts students on the real-world battlefield of cyberspace! It reviews the role that cyberwarfare plays in modern military operations–operations in which it has become almost impossible to separate cyberwarfare from traditional warfare.

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.

Emerging Trends in Information and Communication Security - Günter Müller 2006-06-01

This book constitutes the refereed proceedings of the International Conference on Emerging Trends in Information and Communication Security, ETRICS 2006, held in Freiburg, Germany, in June 2006. The book presents 36 revised full papers, organized in topical sections on multilateral security; security in service-oriented computing, secure mobile applications; enterprise privacy; privacy, identity, and anonymity; security engineering; security policies; security protocols; intrusion detection; and cryptographic security.

Gandhi’s Dharma - Koneru Ramakrishna Rao 2017-09-25

When asked about his message to the world, the Mahatma famously said, ‘My life is my message.’ In him there was no room for contradiction between thought and action. His life in its totality is a series of experiments to convert dharma, moral principles, into karma, practices in action. Gandhi believed that development is a dialectical process stemming from the antinomy of two aspects latent within every individual—the brute and the divine. While the former represents instinct-driven behaviour, the latter is one’s true self, which is altruistic. Gandhi described this process in different fields, most of which are relevant even today. Gandhi’s Dharma is an overview of Mahatma Gandhi—his person, philosophy, and practices. The author asserts that the basic principles governing Gandhi’s thoughts—satya, ahimsa, and sarvodaya—are not relics of the past. Nor are his thoughts an obsolete list of rules. Gandhi’s ideas are dynamic principles perpetually in the making, perfectly adaptable to contemporary life.

Dietary Reference Intakes for Energy, Carbohydrate, Fiber, Fat, Fatty Acids,

Cholesterol, Protein, and Amino Acids - Institute of Medicine 2005-11-28

Responding to the expansion of scientific knowledge about the roles of nutrients in human health, the Institute of Medicine has developed a new approach to establish Recommended Dietary Allowances (RDAs) and other nutrient reference values. The new title for these values Dietary Reference Intakes (DRIs), is the inclusive name being given to this new approach. These are quantitative estimates of nutrient intakes applicable to healthy individuals in the United States and Canada. This new book is part of a series of books presenting dietary reference values for the intakes of nutrients. It establishes recommendations for energy, carbohydrate, fiber, fat, fatty acids, cholesterol, protein, and amino acids. This book presents new approaches and findings which include the following: The establishment of Estimated Energy Requirements at four levels of energy expenditure Recommendations for levels of physical activity to decrease risk of chronic disease The establishment of RDAs for dietary carbohydrate and protein The development of the definitions of Dietary Fiber, Functional Fiber, and Total Fiber The establishment of Adequate Intakes (AI) for Total Fiber The establishment of AIs for linolenic and a-linolenic acids Acceptable Macronutrient Distribution Ranges as a percent of energy intake for fat, carbohydrate, linolenic and a-linolenic acids, and protein Research recommendations for information needed to advance understanding of macronutrient requirements and the adverse effects associated with intake of higher amounts Also detailed are recommendations for both physical activity and energy expenditure to maintain health and decrease the risk of disease.

Building an Effective Cybersecurity Program, 2nd Edition - Tari Schreider 2019-10-22

BUILD YOUR CYBERSECURITY PROGRAM WITH THIS COMPLETELY UPDATED GUIDE Security practitioners now have a comprehensive blueprint to build their cybersecurity programs. Building an Effective Cybersecurity Program (2nd Edition) instructs security architects, security managers, and security engineers how to properly construct effective cybersecurity programs using contemporary architectures, frameworks, and models. This comprehensive book is the result of the author's professional experience and involvement in designing and deploying hundreds of cybersecurity programs. The extensive content includes: Recommended design approaches, Program structure, Cybersecurity technologies, Governance Policies, Vulnerability, Threat and intelligence capabilities, Risk management, Defense-in-depth, DevSecOps, Service management, ...and much more! The book is presented as a practical roadmap detailing each step required for you to build your effective cybersecurity program. It also provides many design templates to assist in program builds and all chapters include self-study questions to gauge your progress. With this new 2nd edition of this handbook, you can move forward confidently, trusting that Schreider is recommending the best components of a cybersecurity program for you. In addition, the book provides hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies. Whether you are a new manager or current manager involved in your organization's cybersecurity program, this book will answer many questions you have on what is involved in building a program. You will be able to get up to speed quickly on program development practices and have a roadmap to follow in building or improving your organization's cybersecurity program. If you are new to cybersecurity in the short period of time it will take you to read this book, you can be the smartest person in the room grasping the complexities of your organization's cybersecurity program. If you are a manager already involved in your organization’s cybersecurity program, you have much to gain from reading this book. This book will become your go to field manual guiding or affirming your program decisions.

Dynamic Business Law: The Essentials - Lucien Dhooge 2012-01-05

Dynamic Business Law: The Essentials is appropriate for the one-semester Business Law course. It contains the basics of business law but does not get bogged down in the kind of details that are more appropriate in an upper-level law class. The text provides an examination of the basic questions, concepts, and legal rules of business law. Emphasis on the BUSINESS in business law. Dynamic Business Law: The Essentials emphasizes the tie of legal issues back to the core business curriculum. This will help both students and faculty. Faculty need to know how this is integrated as they are constantly ‘defending’ the inclusion of this course in the business curriculum. And students need to understand how the concepts tie to their future business careers. Emphasis on TEACHING. Many professors teaching this course are attorneys first and academics second. They do not have a lot of time to prepare or think about how to apply this information effectively for their business students. Dynamic Business Law: The Essentials contains a helpful instructor’s manual, particularly for the many adjuncts teaching this course. Emphasis on CRITICAL THINKING. Neil Browne, one of the co-authors of this text, has written a successful text on critical thinking. His framework is included in Dynamic Business Law: The Essentials as well – to help students learn how to frame and reframe a question/issue. Critical thinking questions are also included at the end of each case, to tie in this component even further.

Making Data Talk - David E. Nelson (M.D.) 2009

The authors summarize and synthesize research on the selection and presentation of data pertinent to public health and provide practical suggestions, based on this research summary and synthesis, on how scientists and other public health practitioners can better communicate data to the public, policy makers and the press.

Legal Issues in Information Security - Joanna Lyn Grama 2011-09

PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES! Legal Issues in Information Security 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. Part 1 of this book discusses fundamental security and privacy concepts. Part 2 examines recent US laws that address information security and privacy. And Part 3 considers security and privacy for organizations.

Cyberethics: Morality and Law in Cyberspace - Richard Spinello 2010-07-06

Revised and updated to reflect new technologies in the field, the fourth edition of this popular text takes an in-depth look at the social costs and moral problems that have emerged by the ever expanding use of the Internet, and offers up-to-date legal and philosophical examinations of these issues. It focuses heavily on content control, free speech, intellectual property, and security while delving into new areas of blogging and social networking. Case studies throughout discuss real-world events and include coverage of numerous hot topics. In the process of exploring current issues, it identifies legal disputes that will likely set the standard for future cases. Instructor Resouces: -PowerPoint Lecture Outlines

The United Nations World Water Development Report - UNESCO World Water Assessment Programme 2021-03-22

Water is a finite and non-substitutable resource. As the foundation of life, societies and economies, it carries multiple values and benefits. But unlike most other natural resources, it has proven extremely difficult to determine its true 'value'. The 2021 edition of the United Nations World Water Development Report, titled "Valuing Water" assesses the current status of and challenges to the valuation of water across different sectors and perspectives and identifies ways in which valuation can be promoted as a tool to help improve its management and achieve global sustainable development.

Christian Ethics: A Guide for the Perplexed - Victor Lee Austin 2012-12-06

Christian ethics is a most perplexing subject. This Guide takes the reader through the most fundamental issues surrounding the question of Ethics from a Christian perspective: Is ethics a meaningful topic of discourse and can there be such a thing as an ethical argument or ethical persuasion? What is the meaning of the adjective in "Christian Ethics"?Could right behavior be different for Christians than it is for others? Can we turn to the Bible for help? Does the Bible tell us what to do, or give us insight into the good we should aim to achieve, or give us a narrative by which to live? Is it best to think of ethics as a matter of duty, or good, or excellence? If we take the virtue line and say that ethics is about human excellence, doing well as a human being or succeeding at being a good human being then what will we say about humans who cannot achieve excellence? The virtue approach leads us to place friendship as the goal of ethics.

Cybersecurity, Cybersecurity, and Cybercrime - Janine Kremling 2017-09-05

Presented from a criminal justice perspective, Cyberspace, Cybersecurity, and Cybercrime introduces students to the interdisciplinary field of cybercrime by exploring the theoretical, practical, and legal framework it operates under, along with strategies to combat it. Authors Janine Kremling and Amanda M. Sharp Parker provide a straightforward overview of cybercrime, cyberthreats, and the vulnerabilities individuals, businesses, and governments face everyday in a digital environment. Highlighting the latest empirical research findings and challenges that cybercrime and cybersecurity pose for those working in the field of criminal justice, this book exposes critical issues related to privacy, terrorism, hacktivism, the dark web, and much more. Focusing on the past, present, and future impact of cybercrime and cybersecurity, it details how criminal justice professionals can be prepared to confront the changing nature of cybercrime.

Legal Issues in Information Security + Case Lab Access - Joanna Lyn Grama 2017-08

Print Textbook & Case Study Lab Access: 180-day subscription. Revised and updated to address the many changes in this evolving field, the Second Edition of Legal Issues in Information Security 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. Labs: Lab 1: Creating an IT Infrastructure Asset List and Identifying Where Privacy Data Resides Lab 2: Case Study on U.S. Veteran Affairs and Loss of Private Information Lab 3: Case Study on PCI DSS Non-

Compliance: CardSystems Solutions Lab 4: Analyzing and Comparing GLBA and HIPAA Lab 5: Case Study on Issues Related to Sharing Consumers' Confidential Information Lab 6: Identifying the Scope of Your State's Data and Security Breach Notification Law Lab 7: Case Study on Digital Millennium Copyright Act: Napster Lab 8: Cyberstalking or Cyberbullying and Laws to Protect Individuals Lab 9: Recommending IT Security Policies to Help Mitigate Risk Lab 10: Case Study on Computer Forensics: Pharmaceutical Company

Managing Risk in Information Systems - Darril Gibson 2014-07-17

This second edition provides a comprehensive overview of the SSCP Risk, Response, and Recovery Domain in addition to providing a thorough overview of risk management and its implications on IT infrastructures and compliance. Written by industry experts, and using a wealth of examples and exercises, this book incorporates hands-on activities to walk the reader through the fundamentals of risk management, strategies and approaches for mitigating risk, and the anatomy of how to create a plan that reduces risk. It provides a modern and comprehensive view of information security policies and frameworks; examines the technical knowledge and software skills required for policy implementation; explores the creation of an effective IT security policy framework; discusses the latest governance, regulatory mandates, business drives, legal considerations, and much more. --

CompTIA Security+ SY0-501 Cert Guide - David L. Prowse 2017-10-18

This is the eBook version of the print title. Note that the eBook may not provide access to the practice test software that accompanies the print book. Access to the companion files are available through product registration at Pearson IT Certification, or see the instructions in the back pages of your eBook. Learn, prepare, and practice for CompTIA Security+ SY0-501 exam success with this CompTIA approved Cert Guide from Pearson IT Certification, a leader in IT certification learning and a CompTIA Authorized Platinum Partner. · Master CompTIA Security+ SY0-501 exam topics · Assess your knowledge with chapter-ending quizzes · Review key concepts with exam preparation tasks · Practice with realistic exam questions CompTIA Security+ SY0-501 Cert Guide is a best-of-breed exam study guide. Best-selling author and expert instructor David L. Prowse shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you with an organized test-preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending chapter review activities help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. Well regarded for its level of detail, assessment features, and challenging review questions and exercises, this CompTIA approved study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time. The CompTIA approved study guide helps you master all the topics on the Security+ exam, including · Core computer system security · OS hardening and virtualization · Application security · Network design elements · Networking ports, protocols, and threats · Network perimeter security · Physical security and authentication models · Access control · Vulnerability and risk assessment · Monitoring and auditing · Cryptography, including PKI · Redundancy and disaster recovery · Social Engineering · Policies and procedures

Policing Democracy - Mark Ungar 2020-03-03

Finally, Policing Democracy probes democratic politics, power relations, and regional disparities of security and reform to establish a framework for understanding the crisis and moving beyond it.

Fundamentals of Communications and Networking - Michael G. Solomon 2014-08-08 Today's networks are required to support an increasing array of real-time communication methods. Video chat, real-time messaging, and always-connected resources put demands on networks that were previously unimagined. The Second Edition of Fundamentals of Communications and Networking helps readers better understand today's networks and the way they support the evolving requirements of different types of organizations. It discusses the critical issues of designing a network that will meet an organization's performance needs and discusses how businesses use networks to solve business problems. Using numerous examples and exercises, this text incorporates hands-on activities to prepare readers to fully understand and design modern networks and their requirements. Key Features of the Second Edition: - Introduces network basics by describing how networks work - Discusses how networks support the increasing demands of advanced communications - Illustrates how to map the right technology to an organization's needs and business goals - Outlines how businesses use networks to solve business problems, both technically and operationally.

Cybersecurity Law - Jeff Kosseff 2019-11-13 The second edition of the definitive guide to cybersecurity law, updated to reflect recent legal developments The revised and updated second edition of Cybersecurity Law offers an authoritative guide to the key statutes, regulations, and court rulings that pertain to cybersecurity. Written by an experienced cybersecurity lawyer and law professor, the second edition includes new and expanded information that reflects the latest changes in laws and regulations. The book includes material on recent FTC data security consent decrees and data breach litigation. Topics covered reflect new laws, regulations, and court decisions that address financial sector cybersecurity, the law of war as applied to cyberspace, and recently updated guidance for public companies' disclosure of cybersecurity risks. This important guide: Provides a new appendix, with 15 edited opinions covering a wide range of cybersecurity-related topics, for students learning via the caselaw method Includes new sections that cover topics such as: compelled access to encrypted devices, New York's financial services cybersecurity regulations, South Carolina's insurance sector cybersecurity law, the Internet of Things, bug bounty programs, the vulnerability equities process, international enforcement of computer hacking laws, the California Consumer Privacy Act, and the European Union's Network and Information Security Directive Contains a new chapter on the critical topic of law of cyberwar Presents a comprehensive guide written by a noted expert on the topic Offers a companion Instructor-only website that features discussion questions for each chapter and suggested exam questions for each chapter Written for students and professionals of cybersecurity, cyber operations, management-oriented information technology (IT), and computer science, Cybersecurity Law, Second Edition is the up-to-date guide that covers the basic principles and the most recent information on cybersecurity laws and regulations. JEFF KOSSEFF is Assistant Professor of Cybersecurity Law at the United States Naval Academy in Annapolis, Maryland. He was a finalist for the Pulitzer Prize, and a recipient of the George Polk Award for national reporting.

Cryptography Decrypted - H. X. Mel 2001

A clear, comprehensible, and practical guide to the essentials of computer cryptography, from Caesar's Cipher through modern-day public key.

Cryptographic capabilities like detecting imposters and stopping eavesdropping are thoroughly illustrated with easy-to-understand analogies, visuals, and historical sidebars. The student needs little or no background in cryptography to read Cryptography Decrypted. Nor does it require technical or mathematical expertise. But for those with some understanding of the subject, this book is comprehensive enough to solidify knowledge of computer cryptography and challenge those who wish to explore the high-level math appendix.

Legal Issues in Information Security - Joanna Grama 2010-10-25

PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES! Legal Issues in Information Security 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. Part 1 of this book discusses fundamental security and privacy concepts. Part 2 examines recent US laws that address information security and privacy. And Part 3 considers security and privacy for organizations.

Recommender Systems Handbook - Francesco Ricci 2015-11-17

This second edition of a well-received text, with 20 new chapters, presents a coherent and unified repository of recommender systems' major concepts, theories, methodologies, trends, and challenges. A variety of real-world applications and detailed case studies are included. In addition to wholesale revision of the existing chapters, this edition includes new topics including: decision making and recommender systems, reciprocal recommender systems, recommender systems in social networks, mobile recommender systems, explanations for recommender systems, music recommender systems, cross-domain recommendations, privacy in recommender systems, and semantic-based recommender systems. This multi-disciplinary handbook involves world-wide experts from diverse fields such as artificial intelligence, human-computer interaction, information retrieval, data mining, mathematics, statistics, adaptive user interfaces, decision support systems, psychology, marketing, and consumer behavior. Theoreticians and practitioners from these fields will find this reference to be an invaluable source of ideas, methods and techniques for developing more efficient, cost-effective and accurate recommender systems.

Rebel Courts - René Provost 2021
Rebel Courts presents an argument that it is possible for non-state armed groups in situations of armed conflict to legally establish and operate a system of courts to administer justice. Neither the concept of the rule of law nor the general principle of state sovereignty stands in the way of framing an understanding of the rule of law adapted to the reality of rebel governance in the area of justice. Legal standards applicable to non-state armed groups in situations of international or non-international armed conflict, including international humanitarian law, international human rights law, and international criminal law, recognise their authority to regularly constitute or establish non-state courts. The lawful operation of such courts is of course subject to requirements of due process, corresponding to an array of guarantees that must be respected in all cases. Rebel courts that are regularly constituted and operate in a manner consistent with due process

guarantees demand a certain degree of recognition by international institutions, by states not involved in the conflict, to some extent by the territorial state, and even by other non-state armed groups. These normative claims are grounded in a series of detailed case studies of the administration of justice by non-state armed groups in a diverse range of conflict situations, including the FARC (Colombia), Islamic State (Syria and Iraq), Taliban (Afghanistan), Tamil Tigers (Sri Lanka), PKK (Turkey), PYD (Syria), and KRG (Iraq).

Cybersecurity for Executives - Gregory J. Touhill 2014-06-09

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

Fast Food Nation - Eric Schlosser 2012

Explores the homogenization of American culture and the impact of the fast food industry on modern-day health, economy, politics, popular culture, entertainment, and food production.

Privacy-Preserving Data Mining - Charu C. Aggarwal 2008-06-10

Advances in hardware technology have increased the capability to store and record personal data. This has caused concerns that personal data may be abused. This book proposes a number of techniques to perform the data mining tasks in a privacy-preserving way. This edited volume contains surveys by distinguished researchers in the privacy field. Each survey includes the key research content as well as future research directions of a particular topic in privacy. The book is designed for researchers, professors, and advanced-level students in computer science, but is also suitable for practitioners in industry.

The Tao of Network Security Monitoring - Richard Bejtlich 2004-07-12

"The book you are about to read will arm you with the knowledge you need to defend your network from attackers—both the obvious and the not so obvious.... If you are new to network security, don't put this book back on the shelf! This is a great book for beginners and I wish I had access to it many years ago. If you've learned the basics of TCP/IP protocols and run an open source or commercial IDS, you may be asking 'What's next?' If so, this book is for you." —Ron Gula, founder and CTO, Tenable Network Security, from the Foreword "Richard Bejtlich has a good perspective on Internet security—one that is orderly and practical at the same time. He keeps readers grounded and addresses the fundamentals in an accessible way." —Marcus Ranum, TruSecure "This book is not about security or network monitoring: It's about both, and in reality these are two aspects of the same problem. You can easily find people who are security experts or network monitors, but this book explains how to master both topics." —Luca Deri, ntop.org "This book will enable security professionals of all skill sets to improve their understanding of what it takes to set up, maintain, and utilize a successful network intrusion detection strategy." —Kirby Kuehl, Cisco Systems Every network can be compromised. There are too many systems, offering too many services, running too many flawed applications. No amount of careful coding, patch management, or access control can keep out every attacker. If prevention eventually fails, how do you prepare for the intrusions that will eventually happen? Network security monitoring (NSM) equips security staff to deal with the inevitable consequences of too few resources and too many responsibilities. NSM collects the data needed to generate better assessment, detection, and response processes—resulting in decreased impact from unauthorized activities. In The Tao of Network Security Monitoring , Richard Bejtlich explores the products, people, and processes that implement the NSM model. By focusing on case studies and the application of open source tools, he helps you gain hands-on knowledge of how to better defend networks and how to mitigate damage from security incidents. Inside, you will find in-depth information on the following areas. The NSM operational framework and deployment considerations. How to use a variety of open-source tools—including Sguil, Argus, and Ethereal—to mine network traffic for full content, session, statistical, and alert data. Best practices for conducting emergency NSM in an incident response scenario, evaluating monitoring vendors, and deploying an NSM architecture. Developing and applying knowledge of weapons, tactics, telecommunications, system administration, scripting, and programming for NSM. The best tools for generating arbitrary packets, exploiting flaws, manipulating traffic, and conducting reconnaissance. Whether you are new to network intrusion detection and incident response, or a computer-security veteran, this book will enable you to quickly develop and apply the skills needed to detect, prevent, and respond to new and emerging threats.

Women Securing the Future with TIPPSS for IoT - Florence D. Hudson 2020-08-14

This book provides insight and expert advice on the challenges of Trust, Identity, Privacy, Protection, Safety and Security (TIPPSS) for the growing Internet of Things (IoT) in our connected world. Contributors cover physical, legal, financial and reputational risk in connected products and services for citizens and institutions including industry, academia, scientific research, healthcare and smart cities. As an important part of the Women in Science and Engineering book series, the work highlights the contribution of women leaders in TIPPSS for IoT, inspiring women and men, girls and boys to enter and apply themselves to secure our future in an increasingly connected world. The book features contributions from prominent female engineers, scientists, business and technology leaders, policy and legal experts in IoT from academia, industry and government. Provides insight into women's contributions to the field of Trust, Identity, Privacy, Protection, Safety and Security (TIPPSS) for IoT Presents information from academia, research, government and industry into advances, applications, and threats to the growing field of cybersecurity and IoT Includes topics such as hacking of IoT devices and systems including healthcare devices, identity and access management, the issues of privacy and your civil rights, and more

Educated - Tara Westover 2018-02-20
#1 NEW YORK TIMES, WALL STREET JOURNAL, AND BOSTON GLOBE BESTSELLER • One of the most acclaimed books of our time: an unforgettable memoir about a young woman who, kept out of school, leaves her survivalist family and goes on to earn a PhD from Cambridge University "Extraordinary . . . an act of courage and self-invention."—The New York Times NAMED ONE OF THE TEN BEST BOOKS OF THE YEAR BY THE NEW YORK TIMES BOOK REVIEW • ONE OF PRESIDENT BARACK OBAMA'S FAVORITE BOOKS OF THE YEAR • BILL GATES'S HOLIDAY READING LIST • FINALIST: National Book Critics Circle's Award In Autobiography and John Leonard Prize For Best First Book • PEN/Jean Stein Book Award • Los Angeles Times Book Prize Born to survivalists in the mountains of Idaho, Tara

Westover was seventeen the first time she set foot in a classroom. Her family was so isolated from mainstream society that there was no one to ensure the children received an education, and no one to intervene when one of Tara's older brothers became violent. When another brother got himself into college, Tara decided to try a new kind of life. Her quest for knowledge transformed her, taking her over oceans and across continents, to Harvard and to Cambridge University. Only then would she wonder if she'd traveled too far, if there was still a way home. "Beautiful and propulsive . . . Despite the singularity of [Westover's] childhood, the questions her book poses are universal: How much of ourselves should we give to those we love? And how much must we betray them to grow up?"—Vogue NAMED ONE OF THE BEST BOOKS OF THE YEAR BY The Washington Post • O: The Oprah Magazine • Time • NPR • Good Morning America • San Francisco Chronicle • The Guardian • The Economist • Financial Times • Newsday • New York Post • theSkimm • Refinery29 • Bloomberg • Self • Real Simple • Town & Country • Bustle • Paste • Publishers Weekly • Library Journal • LibraryReads • Book Riot • Pamela Paul, KQED • New York Public Library

Data Breach and Encryption Handbook - Lucy L. Thomson 2011

This book takes an in-depth look at the issue of escalating data breaches and their legal ramifications. It focuses on the law and its implications, encryption technology, recognized methods of resolving a breach, and many related aspects of information security. The book also examines a number of the major data breach incidents from a variety of legal and technology perspectives, and provides instructive graphics to illustrate the methodologies hackers use to cause these breaches.

Libraries, Telecentres, Cybercafes and Public Access to ICT: International Comparisons - Gomez, Ricardo 2011-07-31

Public venues are vital to information access across the globe, yet few formal studies exist of the complex ways people in developing countries use information technologies in public access places.Libraries, Telecentres, Cybercafes and Public Access to ICT: International Comparisons presents groundbreaking research on the new challenges and opportunities faced by public libraries, community telecentres, and cybercafés that offer public access to computers and other information and communication technologies. Written in plain language, the book presents an in-depth analysis of the spaces that serve underserved populations, bridge "digital divides," and further social and economic development objectives, including employability. With examples and experiences from around the world, this book sheds light on a surprising and understudied facet of the digital revolution at a time when effective digital inclusion strategies are needed more than ever.

System Forensics, Investigation, and Response - John Vacca 2010-09-15

Computer crimes call for forensics specialists---people who know to find and follow the evidence. System Forensics, Investigation, and Response examines the fundamentals of system forensics what forensics is, an overview of computer crime, the challenges of system forensics, and forensics methods. It then addresses the tools, techniques, and methods used to perform computer forensics and investigation, including evidence collection, investigating information-hiding, recovering data, and more. The book closes with an exploration of incident and intrusion response, emerging technologies and future directions of the field, and additional system forensics resources. The Jones & Bartlett Learning Information Systems Security & Assurance Series delivers fundamental IT security principles packed with real world applications and examples for IT Security, Cybersecurity, Information Assurance, and Information

Systems, Security programs. Authored by Certified Information Systems Security professionals (CISSPs), and reviewed by leading technical experts in the field, these books are current, forward-thinking resources that enable readers to solve the cybersecurity challenges of today and tomorrow.

Legal Issues in Information Security - Joanna Lyn Grama 2014-06-19

This revised and updated second edition 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. --

Cybersecurity Law, Standards and Regulations, 2nd Edition - Tari Schreider 2020-02-22

In today's litigious business world, cyber-related matters could land you in court. As a computer security professional, you are protecting your data, but are you protecting your company? While you know industry standards and regulations, you may not be a legal expert. Fortunately, in a few hours of reading, rather than months of classroom study, Tari Schreider's Cybersecurity Law, Standards and Regulations (2nd Edition), lets you integrate legal issues into your security program. Tari Schreider, a board-certified information security practitioner with a criminal justice administration background, has written a much-needed book that bridges the gap between cybersecurity programs and cybersecurity law. He says, "My nearly 40 years in the fields of cybersecurity, risk management, and disaster recovery have taught me some immutable truths. One of these truths is that failure to consider the law when developing a cybersecurity program results in a protective façade or false sense of security." In a friendly style, offering real-world business examples from his own experience supported by a wealth of court cases, Schreider covers the range of practical information you will need as you explore – and prepare to apply – cybersecurity law. His practical, easy-to-understand explanations help you to: Understand your legal duty to act reasonably and responsibly to protect assets and information. Identify which cybersecurity laws have the potential to impact your cybersecurity program. Upgrade cybersecurity policies to comply with state, federal, and regulatory statutes. Communicate effectively about cybersecurity law with corporate legal department and counsel. Understand the implications of emerging legislation for your cybersecurity program. Know how to avoid losing a cybersecurity court case on procedure – and develop strategies to handle a dispute out of court. Develop an international view of cybersecurity and data privacy – and international legal frameworks. Schreider takes you beyond security standards and regulatory controls to ensure that your current or future cybersecurity program complies with all laws and legal jurisdictions. Hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies. This book needs to be required reading before your next discussion with your corporate legal department. This new edition responds to the rapid changes in the cybersecurity industry, threat landscape and providers. It addresses the increasing risk of zero-day attacks, growth of state-sponsored adversaries and consolidation of cybersecurity products and services in addition to the substantial updates of standards, source links and cybersecurity products.

Distributed Computing - Ajay D. Kshemkalyani 2011-03-03

Designing distributed computing systems is a complex process requiring a solid understanding of the design problems and the theoretical and practical aspects of their solutions. This comprehensive textbook covers the fundamental principles and models underlying the theory, algorithms and systems aspects of distributed computing. Broad and detailed coverage of the theory is balanced with practical systems-related issues such as mutual exclusion, deadlock detection, authentication, and failure recovery. Algorithms are carefully selected, lucidly presented, and described without complex proofs. Simple explanations and illustrations are used to elucidate the algorithms. Important emerging topics such as peer-to-peer networks and network security are also considered. With vital algorithms, numerous illustrations, examples and homework problems, this textbook is suitable for advanced undergraduate and graduate students of electrical and computer engineering and computer science. Practitioners in data networking and sensor networks will also find this a valuable resource. Additional resources are available online at www.cambridge.org/9780521876346.

Energetic Food Webs - John C. Moore 2012-05-31

Food webs are viewed as open and dynamic systems.