

[Books] Legal Issues In Information Security Jones Bartlett Learning Information Systems Security Assurance Series

Yeah, reviewing a book **Legal Issues In Information Security Jones Bartlett Learning Information Systems Security Assurance Series** could mount up your near friends listings. This is just one of the solutions for you to be successful. As understood, success does not suggest that you have astonishing points.

Comprehending as without difficulty as settlement even more than supplementary will come up with the money for each success. next to, the proclamation as without difficulty as acuteness of this Legal Issues In Information Security Jones Bartlett Learning Information Systems Security Assurance Series can be taken as well as picked to act.

<p>Legal Issues in Information Security-Director of Dra Operations It Grc and Cybersecurity Programs Educause Joanna Lyn Grama 2014-06-01</p> <p>Part of the Jones & Bartlett Learning Information Systems Security and Assurance Series 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. Instructor Materials for Legal Issues in Information Security include: PowerPoint Lecture Slides Instructor's Guide Sample Course Syllabus Quiz & Exam Questions Case Scenarios/Handouts New to the Second Edition: Includes discussions of amendments in several relevant federal and state laws and regulations since 2011 Reviews relevant court decisions that have come to light since the publication of the first edition Includes numerous information security data breaches highlighting new vulnerabilities*</p> <p><i>Principles of Information Security</i>-Michael E. Whitman 2021-07-06</p>
--

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

Legal Issues in Information Security-Joanna Lyn 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.

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

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

Cybersecurity-Ishaani Priyadarshini 2021-08

"This book is the first of its kind to introduce the integration of ethics, laws, risks, and policies in cyberspace. The book will advance understanding of the ethical and legal aspects of cyberspace followed by the risks involved along with current and proposed cyber policies. This book serves as a summary of the state of the art of cyber laws in the United States and considers more than 50 cyber laws. It also, importantly, incorporates various risk management and security strategies from a number of organizations. Using easy-to-understand language and incorporating case studies, the authors begin with the consideration of ethics and law in cybersecurity and then go on to take into account risks and security policies. The section on risk covers risk identification, risk analysis, risk assessment, risk management, and risk remediation. The very important and exquisite topic of cyber insurance is covered as well-its benefits, types, coverage, etc. The section on cybersecurity policy acquaints readers with the role of policies in cybersecurity and how they are being implemented by means of frameworks. The authors provide a policy overview followed by discussions of several popular cybersecurity frameworks, such as NIST, COBIT, PCI/DSS, ISO series, etc. Each chapter is followed by an overall summary and review that highlights the key points as well as questions for readers to evaluate their understanding based on the chapter content. Cybersecurity: Ethics, Legal, Risks, and Policies is a valuable resource for a large audience that includes instructors, students, professionals in specific fields as well anyone and everyone who is an essential constituent of cyberspace. With increasing cybercriminal activities, it is more important than ever to know the laws and how to secure data and devices"--

Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices-Dudley, Alfreda 2011-09-30

Ethical values in computing are essential for understanding and maintaining the relationship between computing professionals and researchers and the users of their applications and programs. While concerns about cyber ethics and cyber law are constantly changing as technology changes, the intersections of cyber ethics and cyber law are still underexplored. Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices discusses the impact of cyber ethics and cyber law on information technologies and society. Featuring current research, theoretical frameworks, and case studies, the book will highlight the ethical and legal practices used in computing technologies, increase the effectiveness of computing students and professionals in applying ethical values and legal statutes, and provide insight on ethical and legal discussions of real-world applications.

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

Information Security and Privacy-Andrew Serwin 2018

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

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

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.

Security and Privacy From a Legal, Ethical, and Technical Perspective-Christos Kalloniatis 2020-09-09

Understanding and realizing the security and privacy challenges for information systems is a very critical and demanding task for both software engineers and developers to design and implement reliable and trustworthy information systems. This book provides novel contributions and research efforts related to security and privacy by shedding light on the legal, ethical, and technical aspects of security and privacy. This book consists of 12 chapters divided in three groups. The first contains works that discuss the ethical and legal aspects of security and privacy, the second contains works that focus more on the technical aspects of security and privacy, and the third contains works that show the applicability of various solutions in the aforementioned fields. This book is perfect for both experienced readers and young researchers that wish to read about the various aspects of security and privacy.

Legal Issues in Information Security-Joanna Lyn Grama 2014-08-18

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

Privacy and Surveillance Legal Issues-Thomas Reuters 2014-01-01

Privacy and Surveillance Legal Issues provides an authoritative, insiders perspective on helping clients monitor developments and overcome obstacles in information protection. Featuring experienced partners from law firms across the nation, these experts analyze challenges associated with securing data across various industries, and identify ways to help clients defend against cyber attacks. These top lawyers offer specific advice on tailoring security programs according to the type of data involved, assessing client information security based on industry, and applying new protection strategies to meet compliance requirements. From understanding the role of up-and-coming data security programs to helping companies transition to a world of widely-shared information, these experts stress the importance of developing best practices and response plans based on evolving

legal-issues-in-information-security-jones-bartlett-learning-information-systems-security-assurance-series

HITECH Act standards and HIPAA audits. The different niches represented and the breadth of perspectives presented enable readers to get inside some of the great legal minds of today, as these experienced lawyers offer up their thoughts on the keys to success within this dynamic legal field.

National Security Issues in Science, Law, and Technology-Thomas A. Johnson 2016-04-19

The tragedy of 9/11 placed homeland security and the prevention of further attacks into the central focus of our national consciousness. With so many avenues of terror open to our enemies in terms of mode, medium, and location, effective management and mitigation of threat must be grounded in objective risk assessment. The structure of national security decisions should be premised on decision theory and science with minimal political posturing or emotional reactivism. National Security Issues in Science, Law, and Technology demonstrates a mature look at a frightening subject and presents sound, unbiased tools with which to approach any situation that may threaten human lives. By applying the best of scientific decision-making practices this book introduces the concept of risk management and its application in the structure of national security decisions. It examines the acquisition and utilization of all-source intelligence, including the ability to analyze data and forecast patterns, to enable policymakers to make better informed decisions. The text addresses reaction and prevention strategies applicable to chemical, biological, and nuclear weapons; agricultural terrorism; cyberterrorism; and other potential threats to our critical infrastructure. It discusses legal issues that inevitably arise when integrating new legislation with the threads of our Constitution and illustrates the dispassionate analysis of our intelligence, law enforcement, and military operations and actions. Finally, the book considers the redirection of our national research and laboratory system to investigate the very problems terrorists can induce through the use of weapons we have as yet to confront. Taking the guesswork out of hard choices, National Security Issues in Science, Law, and Technology provides anyone burdened with the mantle of responsibility for the protection of the American people with the tools to make sound, well-informed decisions.

Computer Security, Privacy, and Politics -2008-01-01

"This book offers a review of recent developments of computer security, focusing on the relevance and implications of global privacy, law, and politics for society, individuals, and corporations.It compiles timely content on such topics as reverse engineering of software, understanding emerging computer exploits, emerging lawsuits and cases, global and societal implications, and protection from attacks on privacy"--Provided by publisher.

Information Security and Ethics: Concepts, Methodologies, Tools, and Applications-Nemati, Hamid 2007-09-30

Presents theories and models associated with information privacy and safeguard practices to help anchor and guide the development of technologies, standards, and best practices. Provides recent, comprehensive coverage of all issues related to information security and ethics, as well as the opportunities, future challenges, and emerging trends related to this subject.

Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations-Hossein Bidgoli 2006-03-10

The Handbook of Information Security is a definitive 3-volume handbook that offers coverage of both established and cutting-edge theories and developments on information and computer security. The text contains 180 articles from over 200 leading experts, providing the benchmark resource for information security, network security, information privacy, and information warfare.

The Ethics of Cybersecurity-Markus Christen 2020-02-10

This open access book provides the first comprehensive collection of papers that provide an integrative view on cybersecurity. It discusses theories, problems and solutions on the relevant ethical issues involved. This work is sorely needed in a world where cybersecurity has become indispensable to protect trust and confidence in the digital infrastructure whilst respecting fundamental values like equality, fairness, freedom, or privacy. The book has a strong practical focus as it includes case studies outlining ethical issues in cybersecurity and presenting guidelines and other measures to tackle those issues. It is thus not only relevant for academics but also for practitioners in cybersecurity such as providers of security software, governmental CERTs or Chief Security Officers in companies.

Ethical and Social Issues in the Information Age-Joseph M. Kizza 2013-03-09

An introduction to the social and policy issues which have arisen as a result of IT. Whilst it assumes a modest familiarity with computers, the book provides a guide to the issues suitable for undergraduates. In doing so, the author prompts students to consider questions such as: * How do morality and the law relate to each other? * What should be covered in a professional code of conduct for information technology professionals? * What are the ethical issues relating to copying software? * Is electronic monitoring o employees wrong? * What are the moral codes of cyberspace? Throughout, the book shows how in many ways the technological development is outpacing the ability of our legal systems, and how different paradigms applied to ethical questions often proffer conflicting conclusions. As a result, students will find this a thought-provoking and valuable survey of the new and difficult ethical questions posed by the Internet, artificial intelligence, and virtual reality.

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

Managing Risk and Information Security: Protect to Enable, an ApressOpen title, describes the changing risk environment and why a fresh approach to information security is needed. Because almost every aspect of an enterprise is now dependent on technology, the focus of IT security must shift from locking down assets to enabling the business while managing and surviving risk. This compact book discusses business risk from a broader perspective, including privacy and regulatory considerations. It describes the increasing number of threats and vulnerabilities, but also offers strategies for developing solutions. These include discussions of how enterprises can take advantage of new and emerging technologies—such as social media and the huge proliferation of Internet-enabled devices—while minimizing risk. With ApressOpen, content is freely available through multiple online distribution channels and electronic formats with the goal of disseminating professionally edited and technically reviewed content to the worldwide community. Here are some of the responses from reviewers of this exceptional work: “Managing Risk and Information Security is a perceptive, balanced, and often thought-provoking exploration of evolving information risk and security challenges within a business context. Harkins clearly connects the needed, but often-overlooked linkage and dialog between the business and technical worlds and offers actionable strategies. The book contains eye-opening security insights that are easily understood, even by the curious layman.” Fred Wettling, Bechtel Fellow, IS&T Ethics & Compliance Officer, Bechtel “As disruptive technology innovations and escalating cyber threats continue to create enormous information security challenges, Managing Risk and Information Security: Protect to Enable provides a much-needed perspective. This book compels information security professionals to think differently about concepts of risk management in order to be more effective. The specific and practical guidance offers a fast-track formula for developing information security strategies which are lock-step with business priorities.” Laura Robinson, Principal, Robinson Insight Chair, Security for Business Innovation Council (SBIC) Program Director, Executive Security Action Forum (ESAF) “The mandate of the information security function is being completely rewritten. Unfortunately most heads of security haven’t picked up on the change, impeding their companies’ agility and ability to innovate. This book makes the case for why security needs to change, and shows how to get started. It will be regarded as marking the turning point in information security for years to come.” Dr. Jeremy Bergsman, Practice Manager, CEB “The world we are responsible to protect is changing dramatically and at an accelerating pace. Technology is pervasive in virtually every aspect of our lives. Clouds, virtualization and mobile are redefining computing - and they are just the beginning of what is to come. Your security perimeter is defined by wherever your information and people happen to be. We are attacked by professional adversaries who are better funded than we will ever be. We in the information security profession must change as dramatically as the environment we protect. We need new skills and new strategies to do our jobs effectively. We literally need to change the way we think. Written by one of the best in the business, Managing Risk and Information Security challenges traditional security theory with clear examples of the need for change. It also provides expert advice on how to dramatically increase the success of your security strategy and methods - from dealing with the misperception of risk to how to become a Z-shaped CISO. Managing Risk and Information Security is the ultimate treatise on how to deliver effective security to the world we live in for the next 10 years. It is absolute must reading for anyone in our profession - and should be on the desk of every CISO in the world.” Dave Cullinane, CISSP CEO Security Starfish, LLC “In this overview, Malcolm Harkins delivers an insightful survey of the trends, threats, and tactics shaping information risk and security. From regulatory compliance to psychology to the changing threat context, this work provides a compelling introduction to an important topic and trains helpful attention on the effects of changing technology and management practices.” Dr. Mariano-Florentino Cuéllar Professor, Stanford Law School Co-Director, Stanford Center for International Security and Cooperation (CISAC), Stanford University “Malcolm Harkins gets it. In his new book Malcolm outlines the major forces changing the information security risk landscape from a big picture perspective, and then goes on to offer effective methods of managing that risk from a practitioner’s viewpoint. The combination makes this book unique and a must read for anyone interested in IT risk.” Dennis Devinl AVP, Information Security and Compliance, The George Washington University “Managing Risk and Information Security is the first-to-read, must-read book on information security for C-Suite executives. It is accessible, understandable and actionable. No sky-is-falling scare tactics, no techno-babble - just straight talk about a critically important subject. There is no better primer on the economics, ergonomics and psycho-behaviourals of security than this.” Thornton May, Futurist, Executive Director & Dean, IT Leadership Academy “Managing Risk and Information Security is a wake-up call for information security executives and a ray of light for business leaders. It equips organizations with the knowledge required to transform their security programs from a “culture of no” to one focused on agility, value and competitiveness. Unlike other publications, Malcolm provides clear and immediately applicable solutions to optimally balance the frequently opposing needs of risk reduction and business growth. This book should be required reading for anyone currently serving in, or seeking to achieve, the role of Chief Information Security Officer.” Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA “For too many years, business and security - either real or imagined - were at odds. In Managing Risk and Information Security: Protect to Enable, you get what you expect - real life practical ways to break logjams, have security actually enable business, and marries security architecture and business architecture. Why this book? It's written by a practitioner, and not just any practitioner, one of the leading minds in Security today.” John Stewart, Chief Security Officer, Cisco “This book is an invaluable guide to help security professionals address risk in new ways in this alarmingly fast changing environment. Packed with examples which makes it a pleasure to read, the book captures practical ways a forward thinking CISO can turn information security into a competitive advantage for their business. This book provides a new framework for managing risk in an entertaining and thought provoking way. This will change the way security professionals work with their business leaders, and help get products to market faster. The 6 irrefutable laws of information security should be on a stone plaque on the desk of every security professional.” Steven Proctor, VP, Audit & Risk Management, Flextronics

The ABA Cybersecurity Handbook-Jill Deborah Rhodes 2018

With the growing volume of cyberattacks, it is important to ensure you are protected. This handbook will help you to identify potential cybersecurity risks, take steps to lessen those risks, and better respond in the event of an attack. It addresses the current overarching threat, describes how the technology works, outlines key legal requirements and ethical issues, and highlights special considerations for lawyers and practitioners of all types.

Improving Access to and Confidentiality of Research Data-National Research Council 2000-09-11

Improving Access to and Confidentiality of Research Data summarizes a workshop convened by the Committee on National Statistics (CNSTAT) to promote discussion about methods for advancing the often conflicting goals of exploiting the research potential of microdata and maintaining acceptable levels of confidentiality. This report outlines essential themes of the access versus confidentiality debate that emerged during the workshop. Among these themes are the tradeoffs and tensions between the needs of researchers and other data users on the one hand and confidentiality requirements on the other; the relative advantages and costs of data perturbation techniques (applied to facilitate public release) versus restricted access as tools for improving security; and the need to quantify disclosure risks--both absolute and relative--created by researchers and research data, as well as by other data users and other types of data.

Social, Legal, and Ethical Implications of IoT, Cloud, and Edge Computing Technologies-Cornetta, Gianluca 2020-06-26

The adoption of cloud and IoT technologies in both the industrial and academic communities has enabled the discovery of numerous applications and ignited countless new research opportunities. With numerous professional markets benefiting from these advancements, it is easy to forget the non-technical issues that accompany technologies like these. Despite the advantages that these systems bring, significant ethical questions and regulatory issues have become prominent areas of discussion. Social, Legal, and Ethical Implications of IoT, Cloud, and Edge Computing Technologies is a pivotal reference source that provides vital research on the non-technical repercussions of IoT technology adoption. While highlighting topics such as smart cities, environmental monitoring, and data privacy, this publication explores the regulatory and ethical risks that stem from computing technologies. This book is ideally designed for researchers, engineers, practitioners, students, academicians, developers, policymakers, scientists, and educators seeking current research on the sociological

impact of cloud and IoT technologies.

Ethical Issues of Information Systems-Salehnia, Ali 2001-07-01

Understanding, appreciating and taking corrective steps to maintain and enhance social and ethical responsibility in the information age is important not only because of our increased dependence on information and communication technologies, but also because information and communication technologies pose complex challenges. Ethical Issues of Information Systems strives to address these pertinent issues. This scholarly and academic book provides insight on many topics of debate and discussion in the field and lends the most recent research in the field of IT ethics and social responsibility.

Private Security and the Law-Charles Nemeth 2011-10-13

Private Security and the Law, Fourth Edition, is a unique resource that provides a comprehensive analysis of practices in the security industry as they relate to law, regulation, licensure, and constitutional questions of case and statutory authority. It is an authoritative, scholarly treatise that serves as a solid introduction for students regarding the legal and ethical standards that shape the industry. The book takes you step-by-step through the analysis of case law as it applies to situations commonly faced by security practitioners. It describes the legal requirements faced by security firms and emphasizes the liability problems common to security operations, including negligence and tortious liability, civil actions frequently litigated, and strategies to avoid legal actions that affect business efficiency. It also examines the constitutional and due-process dimensions of private security both domestically and internationally, including recent cases and trends that are likely to intensify in the future. New features of this edition include: a chapter on the legal implications of private contractors operating in war zones like Afghanistan; updated coverage of statutory authority, as well as state and federal processes of oversight and licensure; and special analysis of public-private cooperative relationships in law enforcement. A historical background helps readers understand the present by seeing the full context of recent developments. This book will appeal to: students in physical security, security management, and criminal justice programs in traditional and for-profit schools; security professionals; and those working in law enforcement. Authoritative, scholarly treatise sheds light on this increasingly important area of the law Historical background helps readers understand the present by seeing the full context of recent developments National scope provides crucial parameters to security practitioners throughout the US NEW TO THIS EDITION! A chapter on the legal implications of private contractors operating in war zones like Afghanistan, updated coverage of statutory authority, updated coverage of state and federal processes of oversight and licensure, special analysis of public-private cooperative relationships in law enforcement

Global Perspectives In Information Security-Hossein Bidgoli 2008-09-16

Global Perspectives in Information Security, compiled by renowned expert and professor Hossein Bidgoli, offers an expansive view of current issues in information security. Written by leading academics and practitioners from around the world, this thorough resource explores and examines a wide range of issues and perspectives in this rapidly expanding field. Perfect for students, researchers, and practitioners alike, Professor Bidgoli's book offers definitive coverage of established and cutting-edge theory and application in information security.

Legal Regulations, Implications, and Issues Surrounding Digital Data-Jackson, Margaret 2020-06-12

Every year, there are advances in the way that we deal with information as individuals, governments, and organizations. We live and work predominantly online resulting in an enormous amount of digital data. The way that information is used is constantly changing with individuals, governments, and corporations all involved in collecting, storing, using, disclosing, and transferring information online. The growth in artificial intelligence and its effects on data will impact all individuals. It is imperative that a greater understanding of these new advances is gained, in particular, the legal implications they have for society. Legal Regulations, Implications, and Issues Surrounding Digital Data is an essential research publication that assists readers in understanding the current technology they are using, how digital data is being used by governments and organizations, and the current legal issues surrounding these areas that set out challenges in everyday life. Highlighting topics such as data protection, cybercrime, and privacy, this book is ideal for lawyers, academicians, IT specialists, policymakers, cybersecurity professionals, law professionals, researchers, academicians, and students.

Frameworks for ICT Policy: Government, Social and Legal Issues-Adomi, Esharenana E. 2010-07-31

Frameworks for ICT Policy: Government, Social and Legal Issues is a reference on ICT policy framework and a guide to those who are involved in ICT policy formulation, implementation, adoption, monitoring, evaluation and application. This comprehensive publication provides background information for scholars and researchers who are interested in carrying out research on ICT policies and promotes the understanding of policies guiding technology.

The Privacy, Data Protection and Cybersecurity Law Review

Unauthorized Access-Robert H. Sloan 2016-04-19

Going beyond current books on privacy and security, Unauthorized Access: The Crisis in Online Privacy and Security proposes specific solutions to public policy issues pertaining to online privacy and security. Requiring no technical or legal expertise, the book explains complicated concepts in clear, straightforward language. The authors—two renowned experts on computer security and law—explore the well-established connection between social norms, privacy, security, and technological structure. This approach is the key to understanding information security and informational privacy, providing a practical framework to address ethical and legal issues. The authors also discuss how rapid technological developments have created novel situations that lack relevant norms and present ways to develop these norms for protecting informational privacy and ensuring sufficient information security. Bridging the gap among computer scientists, economists, lawyers, and public policy makers, this book provides technically and legally sound public policy guidance about online privacy and security. It emphasizes the need to make trade-offs among the complex concerns that arise in the context of online privacy and security.

Advances in Digital Forensics V-Gilbert Peterson 2009-09-30

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance - investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics V describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: themes and issues, forensic techniques, integrity and privacy, network forensics, forensic computing, investigative techniques, legal issues and evidence management. This book is the fifth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of twenty-three edited papers from the Fifth Annual IFIP WG 11.9 International Conference on Digital Forensics, held at the National Center for Forensic Science, Orlando, Florida, USA in the spring of 2009. Advances in Digital Forensics V is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities.

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

For the Record-National Research Council 1997-07-09

When you visit the doctor, information about you may be recorded in an office computer. Your tests may be sent to a laboratory or consulting physician. Relevant information may be transmitted to your health insurer or pharmacy. Your data may be collected by the state government or by an organization that accredits health care or studies medical costs. By making information more readily available to those who need it, greater use of

computerized health information can help improve the quality of health care and reduce its costs. Yet health care organizations must find ways to ensure that electronic health information is not improperly divulged. Patient privacy has been an issue since the oath of Hippocrates first called on physicians to "keep silence" on patient matters, and with highly sensitive data—genetic information, HIV test results, psychiatric records—entering patient records, concerns over privacy and security are growing. For the Record responds to the health care industry's need for greater guidance in protecting health information that increasingly flows through the national information infrastructure—from patient to provider, payer, analyst, employer, government agency, medical product manufacturer, and beyond. This book makes practical detailed recommendations for technical and organizational solutions and national-level initiatives. For the Record describes two major types of privacy and security concerns that stem from the availability of health information in electronic form: the increased potential for inappropriate release of information held by individual organizations (whether by those with access to computerized records or those who break into them) and systemic concerns derived from open and widespread sharing of data among various parties. The committee reports on the technological and organizational aspects of security management, including basic principles of security; the effectiveness of technologies for user authentication, access control, and encryption; obstacles and incentives in the adoption of new technologies; and mechanisms for training, monitoring, and enforcement. For the Record reviews the growing interest in electronic medical records; the increasing value of health information to providers, payers, researchers, and administrators; and the current legal and regulatory environment for protecting health data. This information is of immediate interest to policymakers, health policy researchers, patient advocates, professionals in health data management, and other stakeholders.

Information Technology Law-Andrew Murray 2016-07-07

Information Technology Law is the ideal companion for a course of study on IT law and the ways in which it is evolving in response to rapid technological and social change. The third edition of this ground-breaking textbook develops its unique examination of the legal processes and their relationship to the modern "information society". Charting the development of the rapid digitization of society and its impact on established legal principles, Murray examines thechallenges faced with enthusiasm and clarity. Following a clearly-defined part structure, the text begins by defining the information society and discussing how it may be regulated, before moving on to explore issues of internet governance, privacy and surveillance, intellectual property and rights,and commerce within the digital sphere. Comprehensive and engaging, Information Technology Law takes an original and thought-provoking approach to examining this fast-moving area of law in context. Online Resource Centre: The third edition is supported by a range of online resources, including:* Additional chapters on the Digital Sphere and Virtual Environments* Audio podcasts suitable for revision* Updates to the law post-publication* A flashcard glossary of key terms and concepts* Outline answers to end of chapter questions* A link to the author's blog, The IT Lawyer* Web links

Modern Theories and Practices for Cyber Ethics and Security Compliance-Yaokumah, Winfred 2020-04-10

In today's globalized world, businesses and governments rely heavily on technology for storing and protecting essential information and data. Despite the benefits that computing systems offer, there remains an assortment of issues and challenges in maintaining the integrity and confidentiality of these databases. As professionals become more dependent cyberspace, there is a need for research on modern strategies and concepts for improving the security and safety of these technologies. Modern Theories and Practices for Cyber Ethics and Security Compliance is a collection of innovative research on the concepts, models, issues, challenges, innovations, and mitigation strategies needed to improve cyber protection. While highlighting topics including database governance, cryptography, and intrusion detection, this book provides guidelines for the protection, safety, and security of business data and national infrastructure from cyber-attacks. It is ideally designed for security analysts, law enforcement, researchers, legal practitioners, policymakers, business professionals, governments, strategists, educators, and students seeking current research on combative solutions for cyber threats and attacks.

The Rise of Big Data Policing-Andrew G. Ferguson 2017-10-03

Winner, 2018 Law & Legal Studies PROSE Award The consequences of big data and algorithm-driven policing and its impact on law enforcement In a high-tech command center in downtown Los Angeles, a digital map lights up with 911 calls, television monitors track breaking news stories, surveillance cameras sweep the streets, and rows of networked computers link analysts and police officers to a wealth of law enforcement intelligence. This is just a glimpse into a future where software predicts future crimes, algorithms generate virtual "most-wanted" lists, and databanks collect personal and biometric information. The Rise of Big Data Policing introduces the cutting-edge technology that is changing how the police do their jobs and shows why it is more important than ever that citizens understand the far-reaching consequences of big data surveillance as a law enforcement tool. Andrew Guthrie Ferguson reveals how these new technologies—viewed as race-neutral and objective—have been eagerly adopted by police departments hoping to distance themselves from claims of racial bias and unconstitutional practices. After a series of high-profile police shootings and federal investigations into systemic police misconduct, and in an era of law enforcement budget cutbacks, data-driven policing has been billed as a way to "turn the page" on racial bias. But behind the data are real people, and difficult questions remain about racial discrimination and the potential to distort constitutional protections. In this first book on big data policing, Ferguson offers an examination of how new technologies will alter the who, where, when and how we police. These new technologies also offer data-driven methods to improve police accountability and to remedy the underlying socio-economic risk factors that encourage crime. The Rise of Big Data Policing is a must read for anyone concerned with how technology will revolutionize law enforcement and its potential threat to the security, privacy, and constitutional rights of citizens. Read an excerpt and interview with Andrew Guthrie Ferguson in The Economist.

Ten Strategies of a World-Class Cybersecurity Operations Center-Carson Zimmerman 2014-07-01

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

Cybersecurity for Executives-Gregory J. Touhill 2014-07-08

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

Cybersecurity Law Fundamentals-Jim Dempsey 2021-07

Network Defense and Countermeasures-William (Chuck) Easttom II 2013-10-18

Everything you need to know about modern network attacks and defense, in one book Clearly explains core network security concepts, challenges, technologies, and skills Thoroughly updated for the latest attacks and countermeasures The perfect beginner's guide for anyone interested in a network security career ¿ Security is the IT industry's hottest topic—and that's where the hottest opportunities are, too. Organizations desperately need professionals who can help them safeguard against the most sophisticated attacks ever created—attacks from well-funded global criminal syndicates, and even governments. ¿ Today, security begins with defending the organizational network. Network Defense and Countermeasures, Second Edition is today's most complete, easy-to-understand introduction to modern network attacks and their effective defense. From malware and DDoS attacks to firewalls and encryption, Chuck Easttom blends theoretical foundations with up-to-the-minute best-practice techniques. Starting with the absolute basics, he discusses crucial topics many security books overlook, including the emergence of network-based espionage and terrorism. ¿ If you have a basic understanding of networks, that's all the background you'll need to succeed with this book: no math or advanced computer science is required. You'll find projects, questions, exercises, case studies, links to expert resources, and a complete glossary—all designed to deepen your understanding and prepare you to defend real-world networks. ¿ Learn how to Understand essential network security concepts, challenges, and careers Learn how modern attacks work Discover how firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs) combine to protect modern networks Select the right security technologies for any network environment Use encryption to protect information Harden Windows and Linux systems and keep them patched Securely configure web browsers to resist attacks Defend against malware Define practical, enforceable security policies Use the "6 Ps" to assess technical and human aspects of system security Detect and fix system vulnerability Apply proven security standards and models, including Orange Book, Common Criteria, and Bell-LaPadula Ensure physical security and prepare for disaster recovery Know your enemy: learn basic hacking, and see how to counter it Understand standard forensic techniques and prepare for investigations of digital crime ¿