Introduction To It Privacy A Handbook For Technologists

This book is about enforcing privacy and data protection. It demonstrates different approaches – regulatory, legal and technological – to enforcing privacy. If regulators do not enforce laws or regulations or codes or do not have the resources, political support or wherewithal to enforce them, they effectively eviscerate and make meaningless such laws or regulations or codes, no matter how laudable or well-intentioned. In some cases, however, the mere existence of such laws or regulations, combined with a credible threat to invoke them, is sufficient for regulatory purposes. But the threat has to be credible. As some of the authors in this book make clear – it is a theme that runs throughout this book – “carrots” and “soft law” need to be backed up by “sticks” and “hard law”. The authors of this book view privacy enforcement as an activity that goes beyond regulatory enforcement, however. In some sense, enforcing privacy is a task that befalls to all of us. Privacy advocates and members of the public can play an important role in combatting the continuing intrusions upon privacy by governments, intelligence agencies and big companies. Contributors to this book - including regulators, privacy advocates, academics, SMEs, a Member of the European Parliament, lawyers and a technology researcher – share their views in the one and only book on Enforcing Privacy.

Some would argue that scarcely a day passes without a new assault on our privacy. In the wake of the whistle-blower Edward Snowden's revelations about the extent of surveillance conducted by the security services in the United States, Britain, and elsewhere, concerns about individual privacy have significantly increased. The Internet generates risks, unimagined even twenty years ago, to the security and integrity of information in all its forms. The manner in which information is collected, stored, exchanged, and used has changed forever; and with it, the character of the threats to individual privacy. The scale of accessible private data generated by the phenomenal growth of blogs, social media, and other contrivances of our information age pose disturbing threats to our privacy. And the hunger for gossip continues to fuel sensationalist media that frequently degrade the notion of a private domain to which we reasonably lay claim. In the new edition of this Very Short Introduction, Raymond Wacks looks at all aspects of privacy to include numerous recent changes, and considers how this fundamental value might be reconciled with competing interests such as security and freedom of expression. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

Introduction to privacy for the IT professional -- Engineering and privacy -- Encryption and other technologies -- Identity and anonymity -- Tracking and surveillance -- Interference -- The roles of governance and risk management in driving a culture of trust.

This textbook draws on academic theory, field research and policy developments to provide an overview of the connections between security and development, before, during and after conflict. This 2nd edition is revised and updated to take account of changes that have occurred in both policy and academic arenas which are relevant to students and practitioners in this area. In an interdependent world it is often argued that the challenges of underdevelopment and insecurity have global implications. This textbook charts an accessible course through these complex debates, providing a comprehensive introduction for those encountering these issues for the first time. The main aims of the revised edition are: • to set out how thinking on conflict, security and development has changed over time and continues to evolve; • to explore the consequences of these changes, particularly for the theory and practice of development and security promotion; • to introduce a range of case studies from across the globe, in order to explore the implications of a combined approach to security and development. The authors are experienced in both the theory and the practice of this field, and illustrate the links between conflict, security and development with practical examples, drawing on key case studies from the past twenty years. Each chapter is informed by student pedagogy and the book will be essential reading for all students of development studies, war and conflict studies, and human security and is recommended for students of international security and IR in general.

Introduction to Machine Learning with Applications in Information Security provides a class-tested introduction to a wide variety of machine learning algorithms, reinforced through realistic applications. The book is accessible and doesn’t prove theorems, or otherwise dwell on mathematical theory. The goal is to present topics at an intuitive level, with just enough detail to clarify the underlying concepts. The book covers core machine learning topics in-depth, including Hidden Markov Models, Principal Component Analysis, Support Vector Machines, and Clustering. It also includes coverage of Nearest Neighbors, Neural Networks, Boosting and AdaBoost, Random Forests, Linear Discriminant Analysis, Vector Quantization, Naive Bayes, Regression Analysis, Conditional Random Fields, and Data Analysis. Most of the examples in the book are drawn from the field of information security, with many of the machine learning applications specifically focused on malware. The applications presented are designed to demystify machine learning techniques by providing straightforward scenarios. Many of the exercises in this book require some programming, and basic computing concepts are assumed in a few of the application sections. However, anyone with a modest amount of programming experience should have no trouble with this aspect of the book. Instructor resources, including PowerPoint slides, lecture videos, and other relevant material are provided on an accompanying website: http://www.cs.sjsu.edu/~stamp/ML/. For the reader’s benefit, the figures in the book are also available in electronic form, and in color. About the Author Mark Stamp has been a Professor of Computer Science at San Jose State University since 2002. Prior to that, he worked at the National Security Agency (NSA) for seven years, and a Silicon Valley startup company for two years. He received his Ph.D. from Texas Tech University in 1992. His love affair with machine learning began in the early 1990s, when he was working at the NSA, and continues today at SJSU, where he has supervised vast numbers of master’s student projects, most of which involve a combination of information security and machine learning.

Professor Raymond Wacks is a leading international expert on privacy. For more than three decades he has published numerous books and articles on this controversial subject. Privacy is a fundamental value that is under attack from several quarters. Electronic surveillance, biometrics, CCTV, ID cards, RFID codes, online security, the monitoring of employees, the uses and misuses of DNA, - to name but a few - all raise fundamental questions about our right to privacy. This Very Short Introduction also analyzes the tension between free speech and privacy generated by intrusive journalism, photography, and gratuitous disclosures by the media of the private lives of celebrities. Professor Wacks concludes this stimulating introduction by

considering the future of privacy in our society. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

Gaining access to high-quality data is a vital necessity in knowledge-based decision making. But data in its raw form often contains sensitive information about individuals. Providing solutions to this problem, the methods and tools of privacy-preserving data publishing enable the publication of useful information while protecting data privacy. Introduction to Privacy-Preserving Data Publishing: Concepts and Techniques presents state-of-the-art information sharing and data integration methods that take into account privacy and data mining requirements. The first part of the book discusses the fundamentals of the field. In the second part, the authors present anonymization methods for preserving information utility for specific data mining tasks. The third part examines the privacy issues, privacy models, and anonymization methods for realistic and challenging data publishing scenarios. While the first three parts focus on anonymizing relational data, the last part studies the privacy threats, privacy models, and anonymization methods for complex data, including transaction, trajectory, social network, and textual data. This book not only explores privacy and information utility issues but also efficiency and scalability challenges. In many chapters, the authors highlight efficient and scalable methods and provide an analytical discussion to compare the strengths and weaknesses of different solutions.

Most introductory texts provide a technology-based survey of methods and techniques that leaves the reader without a clear understanding of the interrelationships between methods and techniques. By providing a strategy-based introduction, the reader is given a clear understanding of how to provide overlapping defenses for critical information. This understanding provides a basis for engineering and risk-management decisions in the defense of information. Information security is a rapidly growing field, with a projected need for thousands of professionals within the next decade in the government sector alone. It is also a field that has changed in the last decade from a largely theory-based discipline to an experience-based discipline. This shift in the field has left several of the classic texts with a strongly dated feel. Provides a broad introduction to the methods and techniques in the field of information security Offers a strategy-based view of these tools and techniques, facilitating selection of overlapping methods for in-depth defense of information Provides very current view of the emerging standards of practice in information security

Since formed in 2002, DHS has been at the forefront of determining and furthering some of the most hotly debated security issues facing the U.S. and global community in the 21st century. Nearly 200 university programs with undergrad and graduate majors have cropped up in the last dozen-plus years with limited resources available to teach from. Homeland Security, Third Edition will continue to serve as the core textbook covering the fundamental history, formation, oversight, and reach of DHS currently. The book is fully updated with new laws, regulations and strategies across intelligence, transportation sectors, emergency management, border security, public utilities and public health.

High-level overview of the information security field. Covers key concepts like confidentiality, integrity, and availability, then dives into practical applications of these ideas in the areas of operational, physical, network, application, and operating system security. In this high-level survey of the information security field, best-selling author Jason Andress covers the basics of a wide variety of topics, from authentication and authorization to maintaining confidentiality and performing penetration testing. Using real-world security breaches as examples, Foundations of Information Security explores common applications of these concepts, such as operations security, network design, hardening and patching operating systems, securing mobile devices, as well as tools for assessing the security of hosts and applications. You'll also learn the basics of topics like: • Multifactor authentication and how biometrics and hardware tokens can be used to harden the authentication process • The principles behind modern cryptography, including symmetric and asymmetric algorithms, hashes, and certificates • The laws and regulations that protect systems and data • Anti-malware tools, firewalls, and intrusion detection systems • Vulnerabilities such as buffer overflows and race conditions A valuable resource for beginning security professionals, network systems administrators, or anyone new to the field, Foundations of Information Security is a great place to start your journey into the dynamic and rewarding field of information security.

A Practical Introduction to Security and Risk Management is the first book to introduce the full spectrum of security and risks and their management. Author and field expert Bruce Newsome helps readers learn how to understand, analyze, assess, control, and generally manage security and risks from the personal to the operational. They will develop the practical knowledge and skills they need, including analytical skills, basic mathematical methods for calculating risk in different ways, and more artistic skills in making judgments and decisions about which risks to control and how to control them. Organized into 16 brief chapters, the book shows readers how to: analyze security and risk; identify the sources of risk (including hazards, threats, and contributors); analyze exposure and vulnerability; assess uncertainty and probability; develop an organization’s culture, structure, and processes congruent with better security and risk management; choose different strategies for managing risks; communicate and review; and manage security in the key domains of operations, logistics, physical sites, information, communications, cyberspace, transport, and personal levels.

This monograph illustrates important notions in security reductions and essential techniques in security reductions for group-based cryptosystems. Using digital signatures and encryption as examples, the authors explain how to program correct security reductions for those cryptographic primitives. Various schemes are selected and re-proven in this book to demonstrate and exemplify correct security reductions. This book is suitable for researchers and graduate students engaged with public-key cryptography.

This student-friendly textbook offers a survey of the competing conceptions and applications of the increasingly prominent notion of environmental security. The book is divided into three sections. In the first, the key theoretical and practical arguments for and against bringing together environmental and security issues are set out. The book then goes on to present how and why environmental issues have come to be framed in some quarters as ‘national security‘ concerns in the context of the effects of overpopulation, resource depletion, climate change and the role of the military as both a cause and a solution to problems of pollution and natural disasters. Finally, the third section explores the case for treating the key issues of environmental change as matters of human security. Overall, the book will provide a clear, systematic and thorough overview of all dimensions of an area of great academic and ‘real-world’ political interest but one

that has rarely been set out in an accessible textbook format hitherto. This book will be essential reading for students of environmental studies, critical and human security, global governance, development studies, and IR in general.

Guides Students in Understanding the Interactions between Computing/Networking Technologies and Security Issues Taking an interactive, "learn-by-doing" approach to teaching, Introduction to Computer and Network Security: Navigating Shades of Gray gives you a clear course to teach the technical issues related to security. Unlike most computer security books, which concentrate on software design and implementation, cryptographic tools, or networking issues, this text also explores how the interactions between hardware, software, and users affect system security. The book presents basic principles and concepts, along with examples of current threats to illustrate how the principles can either enable or neutralize exploits. Students see the importance of these concepts in existing and future technologies. In a challenging yet enjoyable way, they learn about a variety of technical topics, including current security exploits, technical factors that enable attacks, and economic and social factors that determine the security of future systems. Extensively classroom-tested, the material is structured around a set of challenging projects. Through staging exploits and choosing countermeasures to neutralize the attacks in the projects, students learn: How computer systems and networks operate How to reverse-engineer processes How to use systems in ways that were never foreseen (or supported) by the original developers Combining hands-on work with technical overviews, this text helps you integrate security analysis into your technical computing curriculum. It will educate your students on security issues, such as side-channel attacks, and deepen their understanding of how computers and networks work.

Presenting a concise, yet wide-ranging and contemporary overview of the field, this Advanced Introduction to Privacy Law focuses on how we arrived at our privacy laws, and how the law can deal with new and emerging challenges from digital technologies, social networks and public health crises. This illuminating and interdisciplinary book demonstrates how the history of privacy law has been one of constant adaptation to emerging challenges, illustrating the primacy of the right to privacy amidst a changing social and cultural landscape.

Critical Security Studies introduces students to the sub-field through a detailed yet accessible survey of evolving approaches and key issues. This new edition contains two new chapters and has been fully revised and updated. Written in an accessible and clear manner, Critical Security Studies: offers a comprehensive and up-to-date introduction to critical security studies locates critical security studies within the broader context of social and political theory evaluates fundamental theoretical positions within critical security studies in application to key issues. The book is divided into two main parts. The first part, ‘Approaches’, surveys the newly extended and contested theoretical terrain of critical security studies: Critical Theory, Feminism and gender theory, Postcolonialism, Poststructuralism and Securitization theory. The second part, ‘Issues’, then illustrates these various theoretical approaches against the backdrop of a diverse range of issues in contemporary security practices, from environmental, human and homeland security to border security, technology and warfare, and the War against Terrorism. This edition also includes new chapters on Constructivist theories (Part I) and health (Part II). The historical and geographical scope of the book is deliberately broad and readers are introduced to a number of key illustrative case studies. Each of the chapters in Part II concretely illustrate one or more of the approaches discussed in Part I, with clear internal referencing allowing the text to act as a holistic learning tool for students. This book is essential reading for upper-level students of Critical Security Studies, and an important resource for students of International/Global Security, Political Theory and International Relations.

This textbook provides a unique lens through which the myriad of existing Privacy Enhancing Technologies (PETs) can be easily comprehended and appreciated. It answers key privacy-centered questions with clear and detailed explanations. Why is privacy important? How and why is your privacy being eroded and what risks can this pose for you? What are some tools for protecting your privacy in online environments? How can these tools be understood, compared, and evaluated? What steps can you take to gain more control over your personal data? This book addresses the above questions by focusing on three fundamental elements: It introduces a simple classification of PETs that allows their similarities and differences to be highlighted and analyzed; It describes several specific PETs in each class, including both foundational technologies and important recent additions to the field; It explains how to use this classification to determine which privacy goals are actually achievable in a given real-world environment. Once the goals are known, this allows the most appropriate PETs to be selected in order to add the desired privacy protection to the target environment. To illustrate, the book examines the use of PETs in conjunction with various security technologies, with the legal infrastructure, and with communication and computing technologies such as Software Defined Networking (SDN) and Machine Learning (ML). Designed as an introductory textbook on PETs, this book is essential reading for graduate-level students in computer science and related fields, prospective PETs researchers, privacy advocates, and anyone interested in technologies to protect privacy in online environments.

This book offers an accessible overview of the multiple, interdependent issues related to the Women, Peace, and Security (WPS) global agenda. The first introductory overview of the WPS agenda as articulated in multiple national and international resolutions, statements, and initiatives, the book provides a link between the general public and security practitioners to an important but still largely unknown set of global objectives regarding gender equality and long-term peace and stability. Within the context of the changing nature of warfare, and through consideration of empirical evidence, the volume examines the definitions, theoretical underpinnings and methodological challenges associated with WPS. It then discusses with more specificity violence against women, women civilians in war, the role of women in peacemaking, women in the military and in development, and women politicians. The book concludes with a look to the future and number of action items from the macro to the micro level. While challenges and opportunities related to the WPS agenda are global, US policy action and inaction related to WPS and gender equality are provided as examples of what politically needs to be done, has been done, and obstacles to WPS furtherance potentially to be encountered by all countries. This book will be of much interest to students of peace studies, security studies, gender studies and IR.

This book provides the foundations for understanding hardware security and trust, which have become major concerns for national security over the past decade. Coverage includes security and trust issues in all types of electronic devices and systems such as ASICs, COTS, FPGAs, microprocessors/DSPs, and embedded systems. This serves as an invaluable reference to the state-of-the-art research that is of critical significance to the security of, and trust in, modern society’s microelectronic-supported infrastructures.

"If you've got nothing to hide," many people say, "you shouldn't worry about government surveillance." Others argue that we must sacrifice privacy for security. But as Daniel J. Solove argues in this important book, these arguments and many others are flawed. They are based on mistaken views about what it means to protect privacy and the costs and benefits of doing so. The debate between privacy and security has been framed incorrectly as a zero-sum game in which we are forced to choose between one value and the other. Why can't we have both? In this concise and accessible book, Solove exposes the fallacies of many pro-security arguments that have skewed law and policy to favor security at the expense of privacy. Protecting privacy isn't fatal to security measures; it merely involves adequate oversight and regulation. Solove traces the history of the privacy-security debate from the Revolution to the present day. He explains how the law protects privacy and examines concerns with new technologies. He then points out the failings of our current system and offers specific remedies. Nothing to Hide makes a powerful and compelling case for reaching a better balance between privacy and security and reveals why doing so is essential to protect our freedom and democracy"--Jacket.

The subject of international security is never out of the headlines. The subjects of war and peace, military strategy, the proliferation of nuclear weapons and revisionist states remain central to the discussion, but burgeoning concerns such as climate change, migration, poverty, health, and international terrorism have complicated the field. So what really matters? The traditional prioritization of state security or the security needs of individuals, humanity, and the biosphere? And where do the problems lie? Are states themselves as much a part of the problem as the solution for people's security needs? With globalization, the international security environment has become more interdependent than ever before with the establishment of complex networks that make responding to and managing security challenges increasingly difficult, but increasingly necessary. This Very Short Introduction shows that international security is both vibrant and deeply contested, with stakeholders frequently in disagreement over questions of priority and approach. Christopher S. Browning outlines the nature of the key debates about contemporary international security challenges, and discusses the inherent difficulties that exist in tackling them. He also asks to what extent such debates are infused with questions of power, politics, justice, morality, and responsibility. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

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

Security Operations: An Introduction to Planning and Conducting Private Security Details for High-Risk Areas, Second Edition was written for one primary purpose: to keep people alive by introducing them to private security detail tactics and techniques. The book provides an understanding of the basic concepts and rules that need to be followed in protective services, including what comprises good security practice. This second edition is fully updated to include new case scenarios, threat vectors, and new ambush ploys and attack tactics used by opportunistic predators and seasoned threat actors with ever-advanced, sophisticated schemes. Security has always been a necessity for conducting business operations in both low- and high-risk situations, regardless of the threat level in the operating environment. Overseas, those with new ideas or businesses can frequently be targets for both political and criminal threat agents intent on doing harm. Even in the United States, people become targets because of positions held, publicity, politics, economics, or other issues that cause unwanted attention to a person, their family, or business operations. Security Operations, Second Edition provides an introduction to what duties a security detail should perform and how to effectively carry out those duties. The book can be used by a person traveling with a single bodyguard or someone being moved by a full security detail. FEATURES • Identifies what can pose a threat, how to recognize threats, and where threats are most likely to be encountered • Presents individuals and companies with the security and preparedness tools to protect themselves when operating in various environments, especially in high-risk regions • Provides an understanding of operational security when in transit: to vary route selection and keep destinations and movement plans out of the public view • Outlines the tools and techniques needed for people to become security conscious and situationally aware for their own safety and the safety of those close to them An equal help to those just entering the protection business or people and companies that are considering hiring a security detail, Security Operations is a thorough, detailed, and responsible approach to this serious and often high-risk field. Robert H. Deatherage Jr. is a veteran Special Forces Soldier and private security consultant with thirty years’ experience in military and private security operations. His various writings on security topics cover security operations, threat assessment, risk management, client relations, surveillance detection, counter surveillance operations, foot and vehicle movements, and building security—blending solid operational theory with practical field experience.

Because of the rapid growth of cybercrime, cryptography and system security may be the fastest growing technologies in our culture today. This book describes various aspects of cryptography and system security, with a particular emphasis on the use of rigorous security models and practices in the design of networks and systems. The first portion of the book presents the overall system security concepts and provides a general overview of its features, such as object model and inter-object communications. The objective is to provide an understanding of the cryptography underpinnings on which the rest of the book is based. The book is designed to meet the needs of beginners as well as more advanced readers. Features: Covers the major components of cryptography and system security, with a particular emphasis on the use of rigorous security models and practices used in the design of networks and systems Includes a discussion of emerging technologies such as Big Data Analytics, cloud computing, Internet of Things (IoT), Smart Grid, SCADA, control systems, and Wireless Sensor Networks (WSN)

Unlike data communications of the past, today's networks consist of numerous devices that handle the data as it passes from the sender to the receiver. However, security concerns are frequently raised in circumstances where interconnected computers use a network not controlled by any one entity or organization. Introduction to Network Security exam

There are few textbooks available that outline the foundation of security principles while reflecting the modern practices of private security as an industry. Private Security: An Introduction to Principles and Practice takes a new approach to the subject of private sector security that will be welcome addition to the field. The book focuses on the recent history of the industry and the growing dynamic between private sector security and public safety and law enforcement. Coverage will include history and security theory, but emphasis is on current practice, reflecting the technology-driven, fast-paced, global security environment. Such topics covered include a history of the security industry, security law, risk management, physical security, Human Resources and personnel, investigations, institutional and industry-specific security, crisis and emergency planning, critical infrastructure protection, IT and computer security, and more. Rather than being reduced to single chapter coverage, homeland security and terrorism concepts are referenced throughout the book, as appropriate. Currently, it vital that private security entities work with public sector authorities seamlessly—at the state and federal levels—to share information and understand emerging risks and threats. This modern era of security requires an ongoing, holistic focus on the impact and implications of global terror incidents; as such, the book’s coverage of topics consciously takes this approach throughout. Highlights include: Details the myriad changes in security principles, and the practice of private security, particularly since 9/11 Focuses on both foundational theory but also examines current best practices—providing sample forms, documents, job descriptions, and functions—that security professionals must understand to perform and succeed Outlines the distinct, but growing, roles of private sector security companies versus the expansion of federal and state law enforcement security responsibilities Includes key terms, learning objectives, end of chapter questions, Web exercises, and numerous references—throughout the book—to enhance student learning Presents the full range of career options available for those looking entering the field of private security Includes nearly 400 full-color figures, illustrations, and photographs. Private Security: An Introduction to Principles and Practice provides the most comprehensive, up-to-date coverage of modern security issues and practices on the market. Professors will appreciate the new, fresh approach, while students get the most "bang for their buck," insofar as the real-world knowledge and tools needed to tackle their career in the ever-growing field of private industry security. An instructor’s manual with Exam questions, lesson plans, and chapter PowerPoint® slides are available upon qualified course adoption.

Bullock, Haddow, and Coppola have set the standard for homeland security textbooks, and they follow up best-selling third edition with this substantially improved version. As with its predecessor, the book clearly delineates the bedrock principles of preparing for, mitigating, managing, and recovering from emergencies and disasters. However, this new edition emphasizes their value with improved clarity and focus. What's more, it has been thoroughly revised to include changes that are based on transformations relevant to the political, budgetary, and legal aspects of homeland security that have changed since the 2008 Presidential election (and subsequent change in the administration). These include: new chapters on intelligence and counterterrorism, border security, transportation security, and cybersecurity; an expansion of material on the organization of the Department of Homeland Security; strategic and philosophical changes that are recommended and/or that have occurred as a result of the Quadrennial Homeland Security Review completed in 2010; updated budgetary information on both homeland security programs, and on the homeland security grants that have supported safety and security actions at the state and local levels, as well as in the private sector; and changes in the way the public perceives and receives information about security risk, including the possible elimination of the Homeland Security Advisory System. * New chapter that focuses specifically on the border and transportation security missions * An increased focus on cyber security and infrastructure security, both of which are rapidly growing in importance in the homeland security field among officials at all levels * A companion website that includes a full online Instructor's Guide and PowerPoint Lecture Slides.

This uniquely practical introduction to private security emphasizes professionalism and ethics and demonstrates how public law enforcement and private security work in tandem to solve problems and protect both individuals and businesses. INTRODUCTION TO PRIVATE SECURITY focuses on practical, real-world concepts and applications and includes detailed coverage of everything from industry background and related law to premise, retail, business, employment, and information/computer security as well as investigation, surveillance, and even homeland security. Throughout, the emphasis is on providing students with a clear sense of the numerous career opportunities available in this rapidly expanding field -- including real-world insight on how to get a job in private security, concrete information on the skills needed, and succinct overviews of day-to-day job responsibilities. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Introduction to Security has been the leading text on private security for over thirty years. Celebrated for its balanced and professional approach, this new edition gives future security professionals a broad, solid base that prepares them to serve in a variety of positions. Security is a diverse and rapidly growing field that is immune to outsourcing. The author team as well as an outstanding group of subject-matter experts combine their knowledge and experience with a full package of materials geared to experiential learning. As a recommended title for security certifications, and an information source for the military, this is an essential reference for all security professionals. This timely revision expands on key topics and adds new material on important issues in the 21st century environment such as the importance of communication skills; the value of education; internet-related security risks; changing business paradigms; and brand protection. New sections on terrorism and emerging security threats like cybercrime and piracy Top

industry professionals from aerospace and computer firms join instructors from large academic programs as co-authors and contributors Expanded ancillaries for both instructors and students, including interactive web-based video and case studies

This clear and concise new edition offers a comprehensive comparison of national, international, and human security concepts and policies. Laura Neack skillfully argues that security remains elusive because of a centuries-old ethic insisting that states are the primary and most important international actors, that they can rely ultimately only on themselves for protection, and that they must keep all options on the table for national security. This is particularly apparent with the increase in “glocalized” terrorism and the forced migration of millions of people. Although security as a concept can be widened to encompass almost any aspect of existence, Neack focuses especially on security from physical violence. Case studies throughout bring life to the concepts. New cases in this revised edition include the Syrian refugee crisis and the responses from European states, the growth and reach of jihadist terrorist groups and the unilateral and multilateral military actions taken to confront them, drug trafficking organizations and the Mexican government’s failure to protect citizens, the overt use of preventive war by major and regional powers and the increasing American reliance on drone warfare, multilateral "train-and-assist" operations aimed at peacekeeping and counterterrorism in Africa, UN civilian protection mandates in Libya and Côte d’Ivoire and their absence in Syria, and how terrorism and refugee crises are intimately connected. The first edition of this book was published under the title Elusive Security: States First, People Last in 2007.

Big Data Shocks examines the roots of big data, the current climate and rising stars in this world. The book explores the issues raised by big data and discusses theoretical as well as practical approaches to managing information whose scope exists beyond the human scale.

Since the first edition of Security and Loss Prevention was published in 1983, much has changed in security and loss prevention considerations. In the past five years alone, security awareness and the need for added business continuity and preparedness considerations has been uniquely highlighted given events such as Katrina, 9/11, the formation of the Department of Homeland Security, and the increase in world terrorist events. This edition of Security and Loss Prevention is fully updated and encompasses the breadth and depth of considerations involved in implementing general loss prevention concepts and security programs within an organization. The book provides proven strategies to prevent and reduce incidents of loss due to legal issues, theft and other crimes, fire, accidental or intentional harm from employees, as well as the many ramifications of corporate mismanagement. The new edition contains a brand new terrorism chapter, along with coverage on background investigations, protection of sensitive information, internal threats, and considerations at select facilities (nuclear, DoD, government and federal). Author Philip Purpura once again demonstrates why students and professionals alike rely on this best-selling text as a timely, reliable resource. - Covers the latest professional security issues surrounding Homeland Security and risks presented by threats of terrorism - Recommended reading for ASIS International's prestigious CPP Certification - Cases provide real-world applications

Privacy: A Very Short IntroductionOUP Oxford

Today, threats to the security of an organization can come from a variety of sources- from outside espionage to disgruntled employees and internet risks to utility failure. Reflecting the diverse and specialized nature of the security industry, Security: An Introduction provides an up-to-date treatment of a topic that has become increasingly comple

Alan Charles Raul The devastating and reprehensible acts of terrorism committed against the 11, 2001 have greatly affected our lives, our United States on September livelihoods, and perhaps our way of living. The system of government embodied in our Constitution and Bill of Rights was designed to inhibit excessively efficient government. By imposing checks and balances against over-reaching governmental power, the Founders intended to promote the rule of laws, not men - and to protect the prerogatives of citizens over and above their rulers. No faction was to become so powerful that the rights and interests of any other groups or individuals could be easily trampled. Specifically, the Framers of our constitutional structure prohibited the government from suppressing speech, inhibiting the right of free association, of people, conducting unreasonable preventing (peaceful) assemblies searches and seizures, or acting without observing the dictates of due process and fair play. After September 11, there is a risk that the philosophical protections of the Constitution could appear more than a trifle "academic. " Indeed, our tradional notions of "fair play" will be sorely tested in the context of our compelling requirements for effective self-defense against brutal, evil killers who hate the very idea of America. Now that we witness the grave physical dangers that confront our families, friends, neighbors, and businesses, our commitment to limited government and robust individual liberties will of our inevitably - and understandably - be challenged.

This volume examines the relationship between privacy, surveillance and security, and the alleged privacy–security trade-off, focusing on the citizen’s perspective. Recent revelations of mass surveillance programmes clearly demonstrate the ever-increasing capabilities of surveillance technologies. The lack of serious reactions to these activities shows that the political will to implement them appears to be an unbroken trend. The resulting move into a surveillance society is, however, contested for many reasons. Are the resulting infringements of privacy and other human rights compatible with democratic societies? Is security necessarily depending on surveillance? Are there alternative ways to frame security? Is it possible to gain in security by giving up civil liberties, or is it even necessary to do so, and do citizens adopt this trade-off? This volume contributes to a better and deeper understanding of the relation between privacy, surveillance and security, comprising in-depth investigations and studies of the common narrative that more security can only come at the expense of sacrifice of privacy. The book combines theoretical research with a wide range of empirical studies focusing on the citizen’s perspective. It presents empirical research exploring factors and criteria relevant for the assessment of surveillance technologies. The book also deals with the governance of surveillance technologies. New approaches and instruments for the regulation of security technologies and measures are presented, and recommendations for security policies in line with ethics and fundamental rights are discussed. This book will be of much interest to students of surveillance studies, critical security studies, intelligence studies, EU politics and IR in general. A PDF version of this book is available for free in open access via www.tandfebooks.com. It has been made available under

a Creative Commons Attribution-Non Commercial 3.0 license.
Covers: elements of computer security; roles and responsibilities; common threats; computer security policy; computer security program and risk management; security and planning in the computer system life cycle; assurance; personnel/user issues; preparing for contingencies and disasters; computer security incident handling; awareness, training, and education; physical and environmental security; identification and authentication; logical access control; audit trails; cryptography; and assessing and mitigating the risks to a hypothetical computer system.
This major new text provides an accessible yet intellectually rigorous introduction to contemporary Security Studies. It focuses on eight fundamental debates relating to international security, integrating a wide range of empirical issues and theoretical approaches within its critical interrogation of these.
With the end of the Cold War, threats to national security have become increasingly non-military in nature. Issues such as climate change, resource scarcity, infectious diseases, natural disasters, irregular migration, drug trafficking, information security and transnational crime have come to the forefront. This book provides a comprehensive introduction to Non-Traditional Security concepts. It does so by: Covering contemporary security issues in depth Bringing together chapters written by experts in each area Guiding you towards additional material for your essays and exams through further reading lists Giving detailed explanations of key concepts Testing your understanding through end-of-chapter questions Edited by a leading figure in the field, this is an authoritative guide to the key concepts that you'll encounter throughout your non-traditional, and environmental, security studies courses.
Introduction to Cyber Security is a handy guide to the world of Cyber Security. It can serve as a reference manual for those working in the Cyber Security domain. The book takes a dip in history to talk about the very first computer virus, and at the same time, discusses in detail about the latest cyber threats. There are around four chapters covering all the Cyber Security technologies used across the globe. The book throws light on the Cyber Security landscape and the methods used by cybercriminals. Starting with the history of the Internet, the book takes the reader through an interesting account of the Internet in India, the birth of computer viruses, and how the Internet evolved over time. The book also provides an insight into the various techniques used by Cyber Security professionals to defend against the common cyberattacks launched by cybercriminals. The readers will also get to know about the latest technologies that can be used by individuals to safeguard themselves from any cyberattacks, such as phishing scams, social engineering, online frauds, etc. The book will be helpful for those planning to make a career in the Cyber Security domain. It can serve as a guide to prepare for the interviews, exams and campus work.