Information Governance And Security Protecting And Managing Your Company S Proprietary Information

This book's authoritative blend of theory and practice makes it a matchless resource for everyone in the archives and records management field.
Large-scale data loss continues to make headline news, highlighting the need for stringent data protection policies, especially when personal or commercially sensitive information is at stake. This book provides detailed analysis of current data protection laws and discusses compliance issues, enabling the reader to construct a platform on which to build internal compliance strategies. The author is chair of the National Association of Data Protection Officers (NADPO).
Using case studies and hands-on activities, this book discusses topics in information governance (IG): recognizing hidden development and operational implications of IG--and why it needs to be integrated in the broader organization; integrating IG activities with transactional processing, BI, MDM, and other enterprise information management functions; the information governance organization: defining roles, launching projects, and integrating with ongoing operations; performing IG in transactional projects, including those using agile methods and COTS products; bringing stronger information governance to MDM: strategy, architecture, development, and beyond; governing information throughout the BI or big data project lifecycle; performing ongoing IG and data stewardship operational processes; auditing and enforcing data quality management in the context of enterprise information management; maintaining and evolving metadata management for maximum business value. -- $c Edited summary from book.
This book presents the latest research on the challenges and solutions affecting the equilibrium between freedom of speech, freedom of information, information security and the right to informational privacy. Given the complexity of the topics addressed, the book shows how old legal and ethical frameworks may need to be not only updated, but also supplemented and complemented by new conceptual solutions. Neither a conservative attitude ("more of the same") nor a revolutionary zeal ("never seen before") is likely to lead to satisfactory solutions. Instead, more reflection and better conceptual design are needed, not least to harmonise different perspectives and legal frameworks internationally. The focus of the book is on how we may reconcile high levels of information security with robust degrees of informational privacy, also in connection with recent challenges presented by phenomena such as "big data" and security scandals, as well as new legislation initiatives, such as those concerning "the right to be forgotten" and the use of personal data in biomedical research. The book seeks to offer analyses and solutions of the new tensions, in order to build a fair, shareable and sustainable balance in this vital area of human interactions.
Implementing a Program for Securing Confidential Information Assets
Handbook of Research on Knowledge and Organization Systems in Library and Information Science
Securing an IT Organization through Governance, Risk Management, and Audit
Protecting and Managing Your Company's Proprietary Information
Performing Information Governance
Non-Invasive Data Governance
Social Media Analytics, Strategies and Governance
For some small businesses, the security of their information, systems, and networks might not be a high priority, but for their customers, employees, and trading partners it is very important. The size of a small business varies by type of business, but typically is a business or organization with up to 500 employees. In the U.S., the number of small businesses totals to over 95% of all businesses. The small business community produces around 50% of our nation¿s GNP and creates around 50% of all new jobs in our country. Small businesses, therefore, are a very important part of our nation¿s economy. This report will assist small business management to understand how to provide basic security for their information, systems, and networks. Illustrations.
This IBM® Redbooks® publication describes how the IBM Big Data Platform provides the integrated capabilities that are required for the adoption of Information Governance in the big data landscape. As organizations embark on new use cases, such as Big Data Exploration, an enhanced 360 view of customers, or Data Warehouse modernization, and absorb ever growing volumes and variety of data with accelerating velocity, the principles and practices of Information Governance become ever more critical to ensure trust in data and help organizations overcome the inherent risks and achieve the wanted value. The introduction of big data changes the information landscape. Data arrives faster than humans can react to it, and issues can quickly escalate into significant events. The variety of data now poses new privacy and security risks. The high volume of information in all places makes it harder to find where these issues, risks, and even useful information to drive new value and revenue are. Information Governance provides an organization with a framework that can align their wanted outcomes with their strategic management principles, the people who can implement those principles, and the architecture and platform that are needed to support the big data use cases. The IBM Big Data Platform, coupled with a framework for Information Governance, provides an approach to build, manage, and gain significant value from the big data landscape.
Due to changes in the learning and research environment, changes in the behavior of library users, and unique global disruptions such as the COVID-19 pandemic, libraries have had to adapt and evolve to remain up-to-date and responsive to their users. Thus, libraries are adding new, digital resources and services while maintaining most of the old, traditional resources and services. New areas of research and inquiry in the field of library and information science explore the applications of machine learning, artificial intelligence, and other technologies to better serve and expand the library community. The Handbook of Research on Knowledge and Organization Systems in Library and Information Science examines new technologies and systems and their application and adoption within libraries. This handbook provides a global perspective on current and future trends concerning library and information science. Covering topics such as machine learning, library management, ICTs, blockchain technology, social media, and augmented reality, this book is essential for librarians, library directors, library technicians, media specialists, data specialists, catalogers, information resource officers, administrators, IT consultants and specialists, academicians, and students.
A compendium of essential information for the modern security entrepreneur and practitioner The modern security practitioner has shifted from a predominantly protective site and assets manager to a leading contributor to overall organisational resilience. Accordingly, The Security Consultant's Handbook sets out a holistic overview of the essential core knowledge, emerging opportunities and approaches to corporate thinking that are increasingly demanded by employers and buyers in the security market. This book provides essential direction for those who want to succeed in security, either individually or as part of a team. It also aims to stimulate some fresh ideas and provide new market routes for security professionals who may feel that they are underappreciated and overexerted in traditional business domains. Product overview Distilling the author's fifteen years' experience as a security practitioner, and incorporating the results of some fifty interviews with leading security practitioners and a review of a wide range of supporting business literature, The Security Consultant's Handbook provides a wealth of knowledge for the modern security practitioner, covering: Entrepreneurial practice (including business intelligence, intellectual property rights, emerging markets, business funding and business networking)Management practice (including the security function's move from basement to boardroom, fitting security into the wider context of organisational resilience, security management leadership, adding value and professional proficiency)Legislation and regulation (including relevant UK and international laws such as the Human Rights Act 1998, the Data Protection Act 1998 and the Geneva Conventions)Private investigations (including surveillance techniques, tracing missing people, witness statements and evidence, and surveillance and the law)Information and cyber security (including why information needs protection, intelligence and espionage, cyber security threats, and mitigation approaches such as the ISO 27001 standard for information security management)Protective security (including risk assessment methods, person-focused threat assessments, protective security roles, piracy and firearms)Safer business travel (including government assistance, safety tips, responding to crime, kidnapping, protective approaches to travel security and corporate liability)Personal and organisational resilience (including workplace initiatives, crisis management, and international standards such as ISO 22320, ISO 22301 and PAS 200) Featuring case studies, checklists and helpful chapter summaries, The Security Consultant's Handbook aims to be a practical and enabling guide for security officers and contractors. Its purpose is to plug information gaps or provoke new ideas, and provide a real-world support tool for those who want to offer their clients safe, proportionate and value-driven security services. About the author Richard Bingley is a senior lecturer in security and organisational resilience at Buckinghamshire New University, and co-founder of CSARN, the popular business security advisory network. He has more than fifteen years' experience in a range of high-profile security and communications roles, including as a close protection operative at London's 2012 Olympics and in Russia for the 2014 Winter Olympic Games. He is a licensed close protection operative in the UK, and holds a postgraduate certificate in teaching and learning in higher education. Richard is the author of two previous books: Arms Trade: Just the Facts(2003) and Terrorism: Just the Facts (2004).
Safeguarding Critical E-Documents
A Practical Guide
Health Information Governance in a Digital Environment
Information Governance for Healthcare Professionals
Data Protection and Compliance in Context
Secure and protect your Windows environment from cyber threats using zero-trust security principles
Research Anthology on Privatizing and Securing Data
Failure to appreciate the full dimensions of data protection can lead to poor data protection management, costly resource allocation issues, and exposure to unnecessary risks. Data Protection: Governance, Risk Management, and Compliance explains how to gain a handle on the vital aspects of data protection.The author begins by building the foundatio
Proven and emerging strategies for addressing document and records management risk within the framework of information governance principles and best practices Information Governance (IG) is a rapidly emerging "super discipline" and is now being applied to electronic document and records management, email, social media, cloud computing, mobile computing, and, in fact, the management and output of information organization-wide. IG leverages information technologies to enforce policies, procedures and controls to manage information risk in compliance with legal and litigation demands, external regulatory requirements, and internal governance objectives. Information Governance: Concepts, Strategies, and Best Practices reveals how, and why, to utilize IG and leverage information technologies to control, monitor, and enforce information access and security policies. Written by one of the most recognized and published experts on information governance, including specialization in e-document security and electronic records management Provides big picture guidance on the imperative for information governance and best practice guidance on electronic document and records management Crucial advice and insights for compliance and risk managers, operations managers, corporate counsel, corporate records managers, legal administrators, information technology managers, archivists, knowledge managers, and information governance professionals IG sets the policies that control and manage the use of organizational information, including social media, mobile computing, cloud computing, email, instant messaging, and the use of e-documents and records. This extends to e-discovery planning and preparation. Information Governance: Concepts, Strategies, and Best Practices provides step-by-step guidance for developing information governance strategies and practices to manage risk in the use of electronic business documents and records.
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
Practical, step-by-step guidance for corporations, universities and government agencies to protect and secure confidential documents and business records Managers and public officials are looking for technology and information governance solutions to "information leakage" in an understandable, concise format. Safeguarding Critical E-Documents provides a road map for corporations, governments, financial services firms, hospitals, law firms, universities and other organizations to safeguard their internal electronic documents and private communications. Provides practical, step-by-step guidance on protecting sensitive and confidential documents—even if they leave the organization electronically or on portable devices Presents a blueprint for corporations, governments, financial services firms, hospitals, law firms, universities and other organizations to safeguard internal electronic documents and private communications Offers a concise format for securing your organizations from information leakage In light of the recent WikiLeaks revelations, governments and businesses have heightened awareness of the vulnerability of confidential internal documents and communications. Timely and relevant, Safeguarding Critical E-Documents shows how to keep internal documents from getting into the wrong hands and weakening your competitive position, or possible damaging your organization's reputation and leading to costly investigations.
The Path of Least Resistance and Greatest Success
The Information Governance Toolkit
Technologies and Applied Solutions
Concepts, Strategies, and Best Practices
Auditing Information and Cyber Security Governance
IBM Information Governance Solutions
A Practical Approach
The legal obligations placed upon businesses as part of governance requirements makes this essential reading for all businesses, large or small, simple or complex, on and off-line. This is a non-technical and up-to-date explanation of the vital issues facing all companies in an area increasingly noted for the high degrees of unofficial hype alongside government regulation and will be welcomed by those seeking to secure their businesses in the face of sustained threats to their assets and in particular, in relation to their data security. Full of practical and straightforward advice, key areas covered include handling the internet, e-commerce, wireless information systems and the legal and regulatory frameworks.
Organizations, worldwide, have adopted practical and applied approaches for mitigating risks and managing information security program. Considering complexities of a large-scale, distributed IT environments, security should be proactively planned for and prepared ahead, rather than as used as reactions to changes in the landscape. Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions presents high-quality research papers and practice articles on management and governance issues in the field of information security. The main focus of the book is to provide an organization with insights into practical and applied solutions, frameworks, technologies and practices on technological and organizational factors. The book aims to be a collection of knowledge for professionals, scholars, researchers and academicians working in this field that is fast evolving and growing as an area of information assurance.
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 Governance and SecurityProtecting and Managing Your Company's Proprietary InformationButterworth-Heinemann
Protection of Information and the Right to Privacy - A New Equilibrium?
A Step-by-Step Guide to Making Information Governance Work
Protecting Electronic Health Information
A Controls-Based Approach
From the Boardroom to the Keyboard
Information Governance Principles and Practices for a Big Data Landscape
Data Control
For many companies, their intellectual property can often be more valuable than their physical assets. Having an effective IT governance strategy in place can protect this intellectual property, reducing the risk of theft and infringement. Data protection, privacy and breach regulations, computer misuse around investigatory powers are part of a complex and often competing range of requirements to which directors must respond. There is increasingly the need for an overarching information security framework that can provide context and coherence to compliance activity worldwide. IT Governance is a key resource for forward-thinking managers and executives at all levels, enabling them to understand how decisions about information technology in the organization should be made and monitored, and, in particular, how information security risks are best dealt with. The development of IT governance - which recognises the convergence between business practice and IT management - makes it essential for managers at all levels, and in organizations of all sizes, to understand how best to deal with information security risk. The new edition has been full updated to take account of the latest regulatory and technological developments, including the creation of the International Board for IT Governance Qualifications. IT Governance also includes new material on key international markets - including the UK and the US, Australia and South Africa.
Data-governance programs focus on authority and accountability for the management of data as a valued organizational asset. Data Governance should not be about command-and-control, yet at times could become invasive or threatening to the work, people and culture of an organization. Non-Invasive Data Governance™ focuses on formalizing existing accountability for the management of data and improving formal communications, protection, and quality efforts through effective stewarding of data resources. Non-Invasive Data Governance will provide you with a complete set of tools to help you deliver a successful data governance program. Learn how: · Steward responsibilities can be identified and recognized, formalized, and engaged according to their existing responsibility rather than being assigned or handed to people as more work. · Governance of information can be applied to existing policies, standard operating procedures, practices, and methodologies, rather than being introduced or emphasized as new processes or methods. · Governance of information can support all data integration, risk management, business intelligence and master data management activities rather than imposing inconsistent rigor to these initiatives. · A practical and non-threatening approach can be applied to governing information and promoting stewardship of data as a cross-organization asset. · Best practices and key concepts of this non-threatening approach can be communicated effectively to leverage strengths and address opportunities to improve.
Delivering the desired benefits from using information technology in healthcare requires a high degree of data standardization, effective governance and semantic interoperability between systems in the health industry. Corporate chief executive officers (CEOs) and company boards need to be more aware of their governance responsibility. This publication explains these concepts to assist the reader to collaboratively work with others to meet these challenges. With contributions from internationally distinguished authors, this book is a valuable cutting edge resource for anyone working in or for the health industry today and especially for: · Policy and decision makers, · Healthcare professionals, · Health information managers, · Health informaticians and · ICT professionals about: · Data governance. · Semantic interoperability · IT in health care · Information security governance The book is suitable for use as a basic text or reference supporting professional, undergraduate and postgraduate curricula preparing students for practice as health or IT professionals working in today's healthcare system.
If your health care organization is typical, you were successful in getting your electronic medical record (EMR) system installed on time and within budget. You declared victory and collected some money from meaningful use. But very quickly, you realized you were not getting the expected return on your investment. So you started the "optimization"
Information Security Governance

Mastering Windows Security and Hardening
IT Governance
Governance, Risk Management, and Compliance
For the Record
Second Edition
* A practical introduction to the business of management for doctors and managers at all levels * This simple guide provides easy-to-use tools and techniques * It explains jargon presents managerial tasks in context and provides managerial models
The Growing Imperative Need for Effective Information Security Governance With monotonous regularity, headlines announce ever more spectacular failures of information security and mounting losses. The succession of corporate debacles and dramatic control failures in recent years underscores the necessity for information security to be tightly integrated into the fabric of every organization. The protection of an organization's most valuable asset information can no longer be relegated to low-level technical personnel, but must be considered an essential element of corporate governance that is critical to organizational success and survival. Written by an industry expert, Information Security Governance is the first book-length treatment of this important topic, providing readers with a step-by-step approach to developing and managing an effective information security program. Beginning with a general overview of governance, the book covers: The business case for information security Defining roles and responsibilities Developing strategic metrics Determining information security outcomes Setting security governance objectives Establishing risk management objectives Developing a cost-effective security strategy A sample strategy development The steps for implementing an effective strategy Developing meaningful security program development metrics Designing relevant information security management metrics Defining incident management and response metrics Complemented with action plans and sample policies that demonstrate to readers how to put these ideas into practice, Information Security Governance is indispensable reading for any professional who is involved in information security and assurance.
IT Security governance is becoming an increasingly important issue for all levels of a company. IT systems are continuously exposed to a wide range of threats, which can result in huge risks that threaten to compromise the confidentiality, integrity, and availability of information. This book will be of use to those studying information security, as well as those in industry.
Managing information within the enterprise has always been a vital and important task to support the day-to-day business operations and to enable analysis of that data for decision making to better manage and grow the business for improved profitability. To do all that, clearly the data must be accurate and organized so it is accessible and understandable to all who need it. That task has grown in importance as the volume of enterprise data has been growing significantly (analyst estimates of 40 - 50% growth per year are not uncommon) over the years. However, most of that data has been what we call "structured" data, which is the type that can fit neatly into rows and columns and be more easily analyzed. Now we are in the era of "big data." This significantly increases the volume of data available, but it is in a form called "unstructured" data. That is, data from sources that are not as easily organized, such as data from emails, spreadsheets, sensors, video, audio, and social media sites. There is valuable information in all that data but it calls for new processes to enable it to be analyzed. All this has brought with it a renewed and critical need to manage and organize that data with clarity of meaning, understandability, and interoperability. That is, you must be able to integrate this data when it is from within an enterprise but also importantly when it is from many different external sources. What is described here has been and is being done to varying extents. It is called "information governance." Governing this information however has proven to be challenging. But without governance, much of the data can be less useful and perhaps even used incorrectly, significantly impacting enterprise decision making. So we must also respect the needs for information security, consistency, and validity or else suffer the potential economic and legal consequences. Implementing sound governance practices needs to be an integral part of the information control in our organizations. This IBM® Redbooks® publication focuses on the building blocks of a solid governance program. It examines some familiar governance initiative scenarios, identifying how they underpin key governance initiatives, such as Master Data Management, Quality Management, Security and Privacy, and Information Lifecycle Management. IBM Information Management and Governance solutions provide a comprehensive suite to help organizations better understand and build their governance solutions. The book also identifies new and innovative approaches that are developed by IBM practice leaders that can help as you implement the foundation capabilities in your organizations.
Information Governance and Assurance
Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions
Next-Generation Enterprise Security and Governance
A Governance, Risk and Compliance Framework
Cyber Security Management
Records and Information Management
Data Protection, Caldicott, Confidentiality
This two-volume set LNCS 4277/4278 constitutes the refereed proceedings of 14 international workshops held as part of OTM 2006 in Montpellier, France in October/November 2006. The 191 revised full papers presented were carefully reviewed and selected from a total of 493 submissions to the workshops. The first volume begins with 26 additional revised short or poster papers of the OTM 2006 main conferences.
"A much-needed service for society today. I hope this book reaches information managers in the organization now vulnerable to hacks that are stealing corporate information and even holding it hostage for ransom." — Ronald W. Hull, author, poet, and former professor and university administrator A comprehensive entity security program deploys information asset protection through stratified technological and non-technological controls. Controls are necessary for counteracting threats, opportunities, and vulnerabilities risks in a manner that reduces potential adverse effects to defined, acceptable levels. This book presents a methodological approach in the context of normative decision theory constructs and concepts with appropriate reference to standards and the respective guidelines. Normative decision theory attempts to establish a rational framework for choosing between alternative courses of action when the outcomes resulting from the selection are uncertain. Through the methodological application, decision theory techniques can provide objectives determination, interaction assessments, performance estimates, and organizational analysis. A normative model prescribes what should exist according to an assumption or rule.
This comprehensive textbook discusses the legal, organizational and ethical aspects of information governance, assurance and security and their relevance to all aspects of information work. Information governance describes the activities and practices which have developed to control the use of information, including, but not limited to, practices mandated by law. In a world in which information is increasingly seen as a top-level asset, the safeguarding and management of information is of concern to everyone. From the researcher who is responsible for ethical practices in the gathering, analysis, and storage of data, to the reference librarian who must deliver unbiased information; from the records manager who must respond to information requests, to the administrator handling personnel files, this book with equip practitioners and students alike to implement good information governance practice in real-world situations. Key topics covered include: - Information as an asset - The laws and regulations - Data quality management - Dealing with threats - Security, risk management and business continuity - Frameworks, policies, ethics and how it all fits together. Readership: Fully supported by examples, discussion points and practical exercises, this is essential reading for everyone who needs to understand, implement and support information assurance policies and information governance structures. It will be particularly valuable for LIS students taking information management and information governance courses, and information professionals with an advisory or gatekeeping role in information governance within an organization.
Information Governance and Security shows managers in any size organization how to create and implement the policies, procedures and training necessary to keep their organization's most important asset—its proprietary information—safe from cyber and physical compromise. Many intrusions can be prevented if appropriate precautions are taken, and this book establishes the enterprise-level systems and disciplines necessary for managing all the information generated by an organization. In addition, the book encompasses the human element by considering proprietary information lost, damaged, or destroyed through negligence. By implementing the policies and procedures outlined in Information Governance and Security, organizations can proactively protect their reputation against the threats that most managers have never even thought of. Provides a step-by-step outline for developing an information governance policy that is appropriate for your organization Includes real-world examples and cases to help illustrate key concepts and issues Highlights standard information governance issues while addressing the circumstances unique to small, medium, and large companies
Anticipatory Systems: Humans Meet Artificial Intelligence
On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops
Technology's Role in Helping Perfect Health Care Outcomes
OTM Confederated International Conferences and Posters, AWeSOMe, CAMS,COMINF,IS,KSinBIT,MIOS-CIAO,MONET,OnToContent,ORM,PerSys,OTM Academy Doctoral Consortium, RDDS,SWWS,SeBGIS 2006, Montpellier, France, October 29 - November 3, 2006, Proceedings, Part I
The Journey Never Ends
The Security Consultant's Handbook
Computers at Risk
Like other critical organizational assets, information is a strategic asset that requires high level of oversight in order to be able to effectively use it for organizational decision-making, performance improvement, cost management, and risk mitigation. Adopting an information governance program shows a healthcare organization's commitment to managing its information as a valued strategic asset. Information governance serves the dual purpose of optimizing the ability to extract clinical and business value from healthcare information while meeting compliance needs and mitigating risk. Healthcare organizations that have information governance programs will have a competitive edge over others and contributes to safety and quality of care, population health, operational efficiency and effectiveness, and cost reduction initiatives. This is a much-needed book in the healthcare market space. It will explain, in clear terms, how to develop, launch, and oversee an Information Governance program. It also provides advice and insights from leading IG, cybersecurity and information privacy professionals in healthcare.
Social media has spread rapidly on the global stage, driving consumers' attention and influence, both consciously and subconsciously. Whilst this type of platform may have been initially designed as a tool for open communication and expression, it is also being utilized as a digital tool, with widescale use cases. The intelligence explosion, information overload and disinformation play a significant part regarding individual, group and country perceptions. The complex nature of this data explosion created an increasing demand and use of artificial intelligence (AI) and machine learning (ML), to help provide 'big insights' to 'big data'. AI and ML enable the analysis and dissemination of vast amounts of data, however the ungoverned pace at which AI and autonomous systems have been deployed, has created unforeseen problems. Many algorithms and AI systems have been trained on limited or unverified datasets, creating inbuilt and unseen biases. Where these algorithmic tools have been deployed in high impact systems, there are documented occurrences of disastrous decision making and outcomes that have negatively impacted people and communities. Little to no work had been conducted in its vulnerability and ability to exploit AI itself. So, AI and autonomous systems, whilst being a force for societal good, could have the potential to create and exacerbate societies greatest challenges. This is a cohesive volume that addresses challenging problems and presents a range of innovative approaches and discussion.
With the immense amount of data that is now available online, security concerns have been an issue from the start, and have grown as new technologies are increasingly integrated in data collection, storage, and transmission. Online cyber threats, cyber terrorism, hacking, and other cybercrimes have begun to take advantage of this information that can be easily accessed if not properly handled. New privacy and security measures have been developed to address this cause for concern and have become an essential area of research within the past few years and into the foreseeable future. The ways in which data is secured and privatized should be discussed in terms of the technologies being used, the methods and models for security that have been developed, and the ways in which risks can be detected, analyzed, and mitigated. The Research Anthology on Privatizing and Securing Data reveals the latest tools and technologies for privatizing and securing data across different technologies and industries. It takes a deeper dive into both risk detection and mitigation, including an analysis of cybercrimes and cyber threats, along with a sharper focus on the technologies and methods being actively implemented and utilized to secure data online. Highlighted topics include information governance and privacy, cybersecurity, data protection, challenges in big data, security threats, and more. This book is essential for data analysts, cybersecurity professionals, data scientists, security analysts, IT specialists, practitioners, researchers, academicians, and students interested in the latest trends and technologies for privatizing and securing data.
Cyber Security Management: A Governance, Risk and Compliance Framework by Peter Trim and Yang-Im Lee has been written for a wide audience. Derived from research, it places security management in a holistic context and outlines how the strategic marketing approach can be used to underpin cyber security in partnership arrangements. The book is unique because it integrates material that is of a highly specialized nature but which can be interpreted by those with a non-specialist background in the area. Indeed, those with a limited knowledge of cyber security will be able to develop a comprehensive understanding of the subject and will be guided into devising and implementing relevant policy, systems and procedures that make the organization better able to withstand the increasingly sophisticated forms of cyber attack. The book includes a sequence-of-events model; an organizational governance framework; a business continuity management planning framework; a multi-cultural communication model; a cyber security management model and strategic management framework; an integrated governance mechanism; an integrated resilience management model; an integrated management model and system; a communication risk management strategy; and recommendations for counteracting a range of cyber threats. Cyber Security Management: A Governance, Risk and Compliance Framework simplifies complex material and provides a multi-disciplinary perspective and an explanation and interpretation of how managers can manage cyber threats in a pro-active manner and work towards counteracting cyber threats both now and in the future.
Safe Computing in the Information Age
A Practical Development and Implementation Approach
Cybersecurity for Executives
Information Security Governance Simplified
A Business Guide To Information Security
An International Guide to Data Security and ISO27001/ISO27002
Major Challenge for the Digital Society
A comprehensive guide to administering and protecting the latest Windows 11 and Windows server operating system from ongoing cyber threats using zero-trust security principles Key Features Learn to protect your Windows environment using zero-trust and a multi-layered security approach Implement security controls using Intune, Configuration Manager, Defender for Endpoint, and more Understand how to onboard modern cyber-threat defense solutions for Windows clients Book Description Are you looking for the most current and effective ways to protect Windows-based systems from being compromised by intruders? This updated second edition is a detailed guide that helps you gain the expertise to implement efficient security measures and create robust defense solutions using modern technologies. The first part of the book covers security fundamentals with details around building and implementing baseline controls. As you advance, you'll learn how to effectively secure and harden your Windows-based systems through hardware, virtualization, networking, and identity and access management (IAM). The second section will cover administering security controls for Windows clients and servers with remote policy management using Intune, Configuration Manager, Group Policy, Defender for Endpoint, and other Microsoft 365 and Azure cloud security technologies. In the last section, you'll discover how to protect, detect, and respond with security monitoring, reporting, operations, testing, and auditing. By the end of this book, you'll have developed an understanding of the processes and tools involved in enforcing security controls and implementing zero-trust security principles to protect Windows systems. What you will learn Build a multi-layered security approach using zero-trust concepts Explore best practices to implement security baselines successfully Get to grips with virtualization and networking to harden your devices Discover the importance of identity and access management Explore Windows device administration and remote management Become an expert in hardening your Windows infrastructure Audit, assess, and test to ensure controls are successfully applied and enforced Monitor and report activities to stay on top of vulnerabilities Who this book is for If you're a cybersecurity or technology professional, solutions architect, systems engineer, systems administrator, or anyone interested in learning how to secure the latest Windows-based systems, this book is for you. A basic understanding of Windows security concepts, Intune, Configuration Manager, Windows PowerShell, and Microsoft Azure will help you get the best out of this book.
Past events have shed light on the vulnerability of mission-critical computer systems at highly sensitive levels. It has been demonstrated that common hackers can use tools and techniques downloaded from the Internet to attack government and commercial information systems. Although threats may come from mischief makers and pranksters, they are more
This book will address the cybersecurity and cooperate governance challenges associated with enterprises, providing a bigger picture of the concepts, intelligent techniques, practices, and open research directions in this area.
Computers at Risk presents a comprehensive agenda for developing nationwide policies and practices for computer security. Specific recommendations are provided for industry and for government agencies engaged in computer security activities. The volume also outlines problems and opportunities in computer security research, recommends ways to improve the research infrastructure, and suggests topics for investigators. The book explores the diversity of the field, the need to engineer countermeasures based on speculation of what experts think computer attackers may do next, why the technology community has failed to respond to the need for enhanced security systems, how innovators could be encouraged to bring more options to the marketplace, and balancing the importance of security against the right of privacy.

Reducing risk, promoting policy
Information Governance and Security
Information Governance
How to Protect Your Company's IT Assets Reduce Risks and Understand the Law
Small Business Information Security
Data Protection
The Fundamentals

Security practitioners must be able to build a cost-effective security program while at the same time meet the requirements of government regulations. This book lays out these regulations in simple terms and explains how to use the control frameworks to build an effective information security program and governance structure. It discusses how organizations can best ensure that the information is protected and examines all positions from the board of directors to the end user, delineating the role each plays in protecting the security of the organization.