Draft Computer Security Incident Handling Guide

Effective administration of government and governmental organizations is a crucial part of achieving success in those organizations. To develop and implement best practices, policymakers and leaders must first understand the fundamental tenants and recent advances in public administration. Public Affairs and Administration: Concepts, Methodologies, Tools, and Applications explores the concept of governmental management, public policy, and politics at all levels of organizational governance. With chapters on topics ranging from privacy and surveillance to the impact of new media on political participation, this multi-volume reference work is an important resource for policymakers, government officials, and academicians and students of political science.

This book will help IT and business operations managers who have been tasked with addressing security issues. It provides a solid understanding of security incident response and detailed guidance in the setting up and running of specialist incident management teams. Having an incident response plan is required for compliance with government regulations, industry standards such as PCI DSS, and certifications such as ISO 27001. This book will help organizations meet those compliance requirements.

The book discussess the categories of infrastucture that require protection. The issues associated with each, and the responsibilities of the public and private sector in securing this infrastructure.

Strategic Intelligence Management introduces both academic researchers and law enforcement professionals to contemporary issues of national security and information

management and analysis. This contributed volume draws on state-of-the-art expertise from academics and law enforcement practitioners across the globe. The chapter authors provide background, analysis, and insight on specific topics and case studies. Strategic Intelligent Management explores the technological and social aspects of managing information for contemporary national security imperatives. Academic researchers and graduate students in computer science, information studies, social science, law, terrorism studies, and politics, as well as professionals in the police, law enforcement, security agencies, and government policy organizations will welcome this authoritative and wide-ranging discussion of emerging threats. Hot topics like cyber terrorism, Big Data, and Somali pirates, addressed in terms the layperson can understand, with solid research grounding Fills a gap in existing literature on intelligence, technology, and national security

Some fed. agencies, in addition to being subject to the Fed. Information Security Mgmt. Act of 2002, are also subject to similar requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (EPHI). The EPHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. This publication discusses security considerations and resources that may provide value when implementing the requirements of the HIPAA Security Rule. Illustrations.

This companion provides the most comprehensive and up-to-date comparative overview of the cyber-security strategies and doctrines of the major states and actors in Europe, North America, South America, Africa, and Asia. The volume offers an introduction to each nation’s

cyber-security strategy and policy, along with a list of resources in English that may be consulted for those wishing to go into greater depth. Each chapter is written by a leading academic or policy specialist, and contains the following sections: overview of national cyber-security strategy; concepts and definitions; exploration of cyber-security issues as they relate to international law and governance; critical examinations of cyber partners at home and abroad; legislative developments and processes; dimensions of cybercrime and cyberterrorism; implications of cyber-security policies and strategies. This book will be of much interest to students and practitioners in the fields of cyber-security, national security, strategic studies, foreign policy, and international relations.

Computer Security Incident Handling Guide (draft) :.Computer security incident handling guide (draft)recommendations of the National Institute of Standards and TechnologyPrinciples of Incident Response and Disaster RecoveryCengage Learning

Information Security professionals today have to be able to demonstrate their security strategies within clearly demonstrable frameworks, and show how these are driven by their organization's business priorities, derived from sound risk management assessments.This Open Enterprise Security Architecture (O-ESA) Guide provides a valuable reference resource for practising security architects and designers explaining the key security issues, terms, principles, components, and concepts underlying security-related decisions that security architects and designers have to make. In doing so it helps in explaining their security architectures and related decision-making processes to their enterprise architecture colleagues.The description avoids

excessively technical presentation of the issues and concepts, so making it also an eminently digestible reference for business managers - enabling them to appreciate, validate, and balance the security architecture viewpoints along with all the other viewpoints involved in creating a comprehensive enterprise IT architecture.
PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Revised and updated with the latest information from this fast-paced field, Fundamentals of Information System Security, Second Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today. Part 2 is adapted from the Official (ISC)2 SSCP Certified Body of Knowledge and presents a high-level overview of each of the seven domains within the System Security Certified Practitioner certification. The book closes with a resource for readers who desire additional material on information security standards, education, professional certifications, and compliance laws. With its practical, conversational writing style and step-by-step examples, this text is a must-have resource for those entering the world of information systems security. New to the Second Edition: - New material on cloud computing, risk analysis, IP mobility, OMNIBus, and Agile Software Development. - Includes the most recent updates in

Information Systems Security laws, certificates, standards, amendments, and the proposed Federal Information Security Amendments Act of 2013 and HITECH Act. - Provides new cases and examples pulled from real-world scenarios. - Updated data, tables, and sidebars provide the most current information in the field.

Discusses all types of corporate risks and practical means of defending against them. Security is currently identified as a critical area of Information Technology management by a majority of government, commercial, and industrial organizations. Offers an effective risk management program, which is the most critical function of an information security program.

The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules is a comprehensive manual to ensuring compliance with the implementation standards of the Privacy and Security Rules of HIPAA and provides recommendations based on other related regulations and industry best practices. The book is designed to assist you in reviewing the accessibility of electronic protected health information (EPHI) to make certain that it is not altered or destroyed in an unauthorized manner, and that it is available as needed only by authorized individuals for authorized use. It can also help those entities that may not be covered by HIPAA regulations but want to assure their customers they are doing their due diligence to protect their personal and private information. Since HIPAA/HITECH rules generally apply to covered entities, business associates, and their subcontractors, these rules may soon become de facto standards

for all companies to follow. Even if you aren't required to comply at this time, you may soon fall within the HIPAA/HITECH purview. So, it is best to move your procedures in the right direction now. The book covers administrative, physical, and technical safeguards; organizational requirements; and policies, procedures, and documentation requirements. It provides sample documents and directions on using the policies and procedures to establish proof of compliance. This is critical to help prepare entities for a HIPAA assessment or in the event of an HHS audit. Chief information officers and security officers who master the principles in this book can be confident they have taken the proper steps to protect their clients' information and strengthen their security posture. This can provide a strategic advantage to their organization, demonstrating to clients that they not only care about their health and well-being, but are also vigilant about protecting their clients' privacy.

This book provides a comprehensive analysis of the Chinese-Russian bilateral relationship, grounded in a historical perspective, and discusses the implications of the burgeoning 'strategic partnership' between these two major powers for world order and global geopolitics. The volume compares the national worldviews, priorities, and strategic visions for the Chinese and Russian leadership, examining several aspects of the relationship in detail. The energy trade is the most important component of economic ties, although both sides desire to broaden trade and investments. In the military realm, Russia sells advanced arms to China, and the two countries engage in

regular joint exercises. Diplomatically, these two Eurasian powers take similar approaches to conflicts in Ukraine and Syria, and also cooperate on non-traditional security issues including preventing coloured revolutions, cyber management, and terrorism. These issue areas illustrate four themes. Russia and China have common interests that cement their partnership, including security, protecting authoritarian institutions, and re-shaping aspects of the global order. They are key players not only influencing regional issues, but also international norms and institutions. The Sino-Russian partnership presents a potential counterbalance to the United States and democratic nations in shaping the contemporary and emerging geopolitical landscape. Nevertheless, the West is still an important partner for China and Russia. Both seek better relations with the West, but on the basis of 'mutual respect' and 'equality'. Lastly, Russia and China have frictions in their relationship, and not all of their interests overlap. The Sino-Russian relationship has gained considerable momentum, particularly since 2014 as Moscow turned to Beijing attempting to offset tensions with the West in the aftermath of Russia's annexation of Crimea and intervention in Ukraine. However, so far, China and Russia describe their relationship as a comprehensive 'strategic partnership', but they are not 'allies'.

This is the first in a series of three proceedings of the 20th Pacific Basin Nuclear Conference (PBNC). This volume covers the topics of Safety and Security, Public Acceptance and Nuclear Education, as well as Economics and Reducing Cost.

As one in the most important and influential conference series of nuclear science and technology, the 20th PBNC was held in Beijing and the theme of this meeting was “Nuclear: Powering the Development of the Pacific Basin and the World”. It brought together outstanding nuclear scientist and technical experts, senior industry executives, senior government officials and international energy organization leaders from all across the world. The book is not only a good summary of the new developments in the field, but also a useful guideline for the researchers, engineers and graduate students.

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

Servers are frequently targeted by attackers because of the value of their data and services. For example, a server might contain personally identifiable info. that could be used to perform identity theft. This document is intended to assist organizations in installing, configuring, and maintaining secure servers. More specifically, it describes, in detail, the following practices to apply: (1) Securing, installing, and configuring the underlying operating system; (2) Securing, installing, and configuring server software; (3) Maintaining the secure configuration through application of appropriate patches and upgrades, security testing, monitoring of logs, and backups of data and operating system files. Illus.

PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY, 2nd Edition presents methods to identify vulnerabilities within computer networks and the countermeasures that mitigate risks and damage. From market-leading content on contingency planning, to effective techniques that minimize downtime in an emergency, to curbing losses after a breach, this text is the resource needed in case of a network intrusion. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This book constitutes the thoroughly refereed post-conference proceedings of the Third International ICST Conference on e-Infrastructure and e-Services for

Developing Countries, AFRICOMM 2011, held in Zanzibar, Tansania, in November 2011. The 24 revised full papers presented together with 2 poster papers were carefully reviewed and selected from numerous submissions. The papers cover a wide range of topics in the field of information and communication infrastructures. They are organized in two tracks: communication infrastructures for developing countries and electronic services, ICT policy, and regulatory issues for developing countries.

This is the first digital forensics book that covers the complete lifecycle of digital evidence and the chain of custody. This comprehensive handbook includes international procedures, best practices, compliance, and a companion web site with downloadable forms. Written by world-renowned digital forensics experts, this book is a must for any digital forensics lab. It provides anyone who handles digital evidence with a guide to proper procedure throughout the chain of custody--from incident response through analysis in the lab. A step-by-step guide to designing, building and using a digital forensics lab A comprehensive guide for all roles in a digital forensics laboratory Based on international standards and certifications

The urgency for a global standard of excellence for those who protect the networked world has never been greater. (ISC)2 created the information security industry's first and only CBK, a

global compendium of information security topics. Continually updated to incorporate rapidly changing technologies and threats, the CBK conti

The present work will discuss relevant theoretical frameworks and applications pertaining to enabling resilience within the risk, crisis and disaster management domain. The contributions to this book focus on resilience thinking along 4 broad themes: Urban Domain; Cyber Domain; Organizational/Social domain; and Socio-ecological domain. This book would serve as a valuable reference for courses on risk, crisis and disaster management, international development, social innovation and resilience. This will be of particular interest to those working in the risk, crisis and disaster management domain as it will provide valuable insights into enabling resilience. This book will be well positioned to inform disaster management professionals, policy makers and academics on strategies and perspectives regarding disaster resilience.

CyberWar, CyberTerror, CyberCrime provides a stark and timely analysis of the increasingly hostile online landscape that today's corporate systems inhabit, and gives a practical introduction to the defensive strategies that can be employed in response.

If a network is not secure, how valuable is it? Introduction to Computer Networks and Cybersecurity takes an integrated approach to networking and cybersecurity, highlighting the interconnections so that you quickly understand the complex design issues in modern networks. This full-color book uses a wealth of examples and illustrations to effective

NIST SP 1800-3A & 3B Second Draft 20 September 2017 Printed in COLOR NIST approach uses commercially available products that can be included alongside your current products in your existing infrastructure. This example solution is packaged as a "How To" guide that

demonstrates implementation of standards-based cybersecurity technologies in the real world. It can save organizations research and proof-of-concept costs for mitigating risk through the use of context for access decisions. Includes a list of applicable NIST, UFC, and MIL-HDBK cybersecurity publications for consideration. Why buy a book you can download for free? First you gotta find a good clean (legible) copy and make sure it''s the latest version (not always easy). Some documents found on the web are missing some pages or the image quality is so poor, they are difficult to read. We look over each document carefully and replace poor quality images by going back to the original source document. We proof each document to make sure it''s all there - including all changes. If you find a good copy, you could print it using a network printer you share with 100 other people (typically its either out of paper or toner). If it''s just a 10-page document, no problem, but if it''s 250-pages, you will need to punch 3 holes in all those pages and put it in a 3-ring binder. Takes at least an hour. It''s much more cost-effective to just order the latest version from Amazon.com This book is published by 4th Watch Books and includes copyright material. We publish compact, tightly-bound, full-size books (8 by 11 inches), with glossy covers. 4th Watch Books is a Service Disabled Veteran-Owned Small Business (SDVOSB). If you like the service we provide, please leave positive review on Amazon.com. For more titles published by 4th Watch Books, please visit: cybah.webplus.net NIST SP 800-12 An Introduction to Information Security NIST SP 800-18 Developing Security Plans for Federal Information Systems NIST SP 800-31 Intrusion Detection Systems NIST SP 800-34 Contingency Planning Guide for Federal Information Systems NIST SP 800-35 Guide to Information Technology Security Services NIST SP 800-39 Managing Information Security Risk NIST SP 800-40 Guide to Enterprise Patch Management Technologies NIST SP 800-41

Guidelines on Firewalls and Firewall Policy NIST SP 800-44 Guidelines on Securing Public Web Servers NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems NIST SP 800-48 Guide to Securing Legacy IEEE 802.11 Wireless Networks NIST SP 800-53A Assessing Security and Privacy Controls NIST SP 800-61 Computer Security Incident Handling Guide NIST SP 800-77 Guide to IPsec VPNs NIST SP 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops NIST SP 800-92 Guide to Computer Security Log Management NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) NIST SP 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i NIST SP 800-137 Information Security Continuous Monitoring (ISCM) NIST SP 800-160 Systems Security Engineering NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems NIST SP 1800-7 Situational Awareness for Electric Utilities NISTIR 7628 Guidelines for Smart Grid Cybersecurity DoD Energy Manager''s Handbook FEMP Operations & Maintenance Best Practices UFC 4-020-01 UFC 4-021-02 Draft NISTIR 8179 Criticality Analysis Process Model

The Official (ISC)2® Guide to the CISSP®-ISSEP® CBK® provides an inclusive analysis of all of the topics covered on the newly created CISSP-ISSEP Common Body of Knowledge. The first fully comprehensive guide to the CISSP-ISSEP CBK, this book promotes understanding of the four ISSEP domains: Information Systems Security Engineering (ISSE); Certification and Accreditation; Technical Management; and an Introduction to United States Government Information Assurance Regulations. This volume explains ISSE by comparing it to a traditional Systems Engineering model, enabling you to see the correlation of how security fits into the design and development process for information systems. It also details key points of more

than 50 U.S. government policies and procedures that need to be understood in order to understand the CBK and protect U.S. government information. About the Author Susan Hansche, CISSP-ISSEP is the training director for information assurance at Nortel PEC Solutions in Fairfax, Virginia. She has more than 15 years of experience in the field and since 1998 has served as the contractor program manager of the information assurance training program for the U.S. Department of State.

Data security and privacy law continues to evolve at a rapid pace, resulting in many compliance pitfalls beyond traditional laws and regulations. Most institutions are not able to keep up. Is yours? Despite the amount of legislation, regulation and litigation, the handling and security of data is still in the early stages of development, where groundbreaking initiatives continue to occur. With the rising influx of jurisdictional issues, which are confusing at best and often contradictory, having a complete analysis of the legal treatment of major issues is key. That's what Data Privacy, Protection and Security Law is here to do, bringing you the key opinions from outstanding legal experts, rather than another recitation of the law. Data Privacy, Protection and Security Law: • Lays out all legal liability issues regarding privacy in an easily accessible, eBook format • Provides a complete analysis of legal treatments, with commentary from our expert authors • Examines whether and how the courts, regulators and parties

make the correct judgments • Gives legal context for business planning in connection with data privacy and security compliance • Includes periodic updates to keep you informed on the latest developments in data privacy and security law In depth topics covered include: • Data protection laws • Selected e-commerce privacy issues • Identity theft • Personal data security: Issues in Law • Data security and wrongdoer's liability • Voluntary obligations to third parties • Obligations imposed in Law • And other data security issues! The authors are the top experts in e-commerce law. Raymond T. Nimmer is the Dean and the Leonard Childs professor of law at the University of Houston Law Center, where he also codirects the Intellectual Property and Information Law Institute. He was reporter for the Uniform Computer Information Transactions Act, and is internationally acclaimed as an expert on electronic commerce law. Holly K. Towle is the cross-firm coordinator of the E-Merging Commerce practice group at K&L Gates (Kirkpatrick & Lockhart, Preston Gates Ellis LLP). She is one of the world's most respected authorities on Internet-based transactions and banking law. Together they provide authoritative analyses of all the different issues facing those transacting e-commerce, including rights, licenses, liabilities, and compliance.

This book provides use case scenarios of machine learning, artificial intelligence,

and real-time domains to supplement cyber security operations and proactively predict attacks and preempt cyber incidents. The authors discuss cybersecurity incident planning, starting from a draft response plan, to assigning responsibilities, to use of external experts, to equipping organization teams to address incidents, to preparing communication strategy and cyber insurance. They also discuss classifications and methods to detect cybersecurity incidents, how to organize the incident response team, how to conduct situational awareness, how to contain and eradicate incidents, and how to cleanup and recover. The book shares real-world experiences and knowledge from authors from academia and industry.

Fed. agencies are facing a set of cybersecurity threats that are the result of increasingly sophisticated methods of attack & the blending of once distinct types of attack into more complex & damaging forms. Examples of these threats include: spam (unsolicited commercial e-mail), phishing (fraudulent messages to obtain personal or sensitive data), & spyware (software that monitors user activity without user knowledge or consent). This report determines: the potential risks to fed. systems from these emerging cybersecurity threats; the fed. agencies' perceptions of risk & their actions to mitigate them, fed. & private-sector actions to address the threats on a nat. level; & governmentwide challenges to protecting

fed. systems from these threats. Illus.