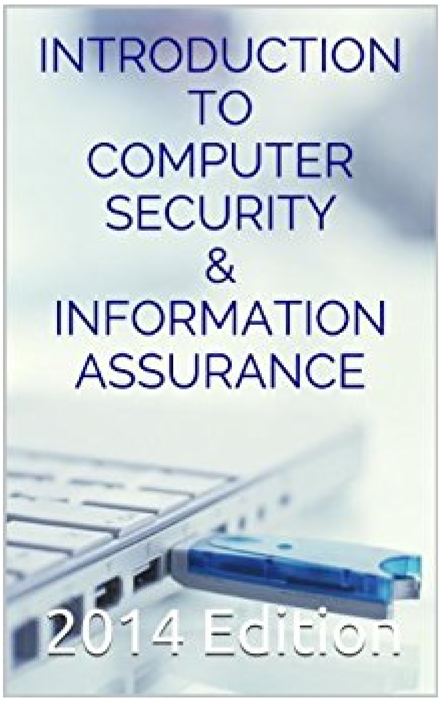
Introduction To Computer Security And Information Assurance



Synopsis

This book is now available as part of The Big Computer Science Book Bundle. Get more for less. About This book will provide you with a not-too-technical guide for information security; weÃ¢â ¬â„¢ll cover everything from social engineering to cyber warfare. This book is right for anyone who wants to know more about information assurance (security), you wonÃ¢â ¬â„¢t need any prior experience in the field as this book is an introduction and aims to get you up to speed in the information security field. ContentsIn chapter 1 we start off by discussing the basic concepts on information assurance, weÃ¢â ¬â„¢ll talk about the meaning of information, a little about risk, security goals and who might want to attack us. In chapter 2 we go onto looking at the various types of attacks we may face. In chapter 3 we discuss the three security goals in more detail, look at the advantages and disadvantages of offensive and defensive security and compare the various security models most widely used today. Chapter 4 is concerned with how we measure risk and how we mitigate it through the use of standards. Chapter 5 discusses possible business constraints, the economy and the problem of security and itÃ¢â ¬â„¢s cost.In chapter 6 we discuss some of the security technologies we can put in place to mitigate the attacks from chapter 2. Chapter 7 explains the Ã¢â ¬Ëœhuman problemÃ¢â ¬â„¢ in security and how your staff are often your biggest vulnerability. In chapter 8 we look at the differences between personal, business and government data and the issues each face. In chapter 9 we move onto looking at the different policies commonly put in place and best practices for the industry. Chapter 10 discusses how we can put better controls in place, build a business continuity plan and try mitigating some of the risks. Chapter 11 is concerned with the law, however we recognise IT professionals are not lawyers so we only step through a general overview of some relevant acts. Chapter 12 is concerned with the forensics side of the industry, collecting data and presenting it in court; along with the challenges computer forensic analysisÃ¢â ¬â„¢s face. We then move onto looking at incident response in chapter 13, how to keep the businesses running even after a disaster. Finally we consider cyber warfare in chapter 14.

Book Information

File Size: 682 KB

Print Length: 100 pages

Publication Date: April 30, 2014

Sold by:Ã Â Digital Services LLC

Language: English

ASIN: B00K2AXZJ6

Text-to-Speech: Enabled

X-Ray: Not Enabled

Word Wise: Enabled

Lending: Not Enabled

Screen Reader: Supported

Enhanced Typesetting: Enabled

Best Sellers Rank: #1,093,369 Paid in Kindle Store (See Top 100 Paid in Kindle Store) #35 inÃ Â Kindle Store > Kindle eBooks > Business & Money > Economics > Commercial Policy #89 inÃ Â Books > Business & Money > Economics > Commercial Policy #1423 inÃ Â Kindle Store > Kindle eBooks > Computers & Technology > Security & Encryption

Download to continue reading...

Fundamentals Of Information Systems Security (Information Systems Security & Assurance) - Standalone book (Jones & Bartlett Learning Information Systems Security & Assurance) Introduction to Computer Security and Information Assurance Social Security & Medicare Facts 2016: Social Security Coverage, Maximization Strategies for Social Security Benefits, Medicare/Medicaid, Social Security Taxes, Retirement & Disability, Ser Human Systems Integration to Enhance Maritime Domain Awareness for Port/Harbour Security: Volume 28 NATO Science for Peace and Security Series - D: ... D: Information and Communication Security) Auditing & Assurance Services (Auditing and Assurance Services) ISO/IEC 27002:2013, Second Edition: Information technology Security techniques Code of practice for information security controls ISO/IEC 27001:2013, Second Edition: Information technology - Security techniques - Information security management systems - Requirements ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management (Redesignation of ISO/IEC 17799:2005) ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century: Computer Crimes, Laws, and Policing in the 21st Century (Praeger Security International) 1st Grade Computer Basics : The Computer and Its Parts: Computers for Kids First Grade (Children’s Computer Hardware Books) Digital Logic Design and Computer Organization with Computer Architecture for Security Hacking: Computer Hacking, Security Testing, Penetration Testing, and Basic Security Hacking: How to Hack Computers, Basic Security and Penetration Testing (Hacking, How to Hack, Hacking for Dummies, Computer Hacking, penetration testing, basic security, arduino, python) Nuclear Safeguards, Security and Nonproliferation:

Achieving Security with Technology and Policy (Butterworth-Heinemann Homeland Security) Security, Rights, & Liabilities in E-Commerce (Artech House Computer Security Series) Security Camera For Home: Learn Everything About Wireless Security Camera System, Security Camera Installation and More Computer Viruses and Malware (Advances in Information Security) Formal Correctness of Security Protocols (Information Security and Cryptography) Security Risk Management: Building an Information Security Risk Management Program from the Ground Up