Information Assurance Handbook: Effective Computer Security And Risk Management Strategies
Synopsis

Best practices for protecting critical data and systems Information Assurance Handbook: Effective Computer Security and Risk Management Strategies discusses the tools and techniques required to prevent, detect, contain, correct, and recover from security breaches and other information assurance failures. This practical resource explains how to integrate information assurance into your enterprise planning in a non-technical manner. It leads you through building an IT strategy and offers an organizational approach to identifying, implementing, and controlling information assurance initiatives for small businesses and global enterprises alike. Common threats and vulnerabilities are described and applicable controls based on risk profiles are provided. Practical information assurance application examples are presented for select industries, including healthcare, retail, and industrial control systems. Chapter-ending critical thinking exercises reinforce the material covered. An extensive list of scholarly works and international government standards is also provided in this detailed guide. Comprehensive coverage includes: Basic information assurance principles and concepts Information assurance management system Current practices, regulations, and plans Impact of organizational structure Asset management Risk management and mitigation Human resource assurance Advantages of certification, accreditation, and assurance Information assurance in system development and acquisition Physical and environmental security controls Information assurance awareness, training, and education Access control Information security monitoring tools and methods Information assurance measurements and metrics Incident handling and computer forensics Business continuity management Backup and restoration Cloud computing and outsourcing strategies Information assurance big data concerns

Book Information

File Size: 20572 KB
Print Length: 480 pages
Publisher: McGraw-Hill Education; 1 edition (September 12, 2014)
Publication Date: September 12, 2014
Sold by: Digital Services LLC
Language: English
ASIN: B00LI364GW
Text-to-Speech: Enabled
X-Ray: Not Enabled
Word Wise: Not Enabled
Schou, Corey, and Steven Hernandez. Information Assurance Handbook - Effective Computer Security and Risk Management. New York: McGraw Hill Education, 2015. This is a well-conceived and well-executed reference for both business/government leaders, computer security, information assurance (IA) professionals who want a timely review and critical discussion of the range of threats and IA principles/methods to meet the challenges to today’s IT systems. The book offers some practical frameworks and methodologies for approaching both legacy and emerging information technologies such as data-mining, cloud-based, client/server applications, all toward the focus of achieving and sustaining competitive advantage. This book is exemplary about in the dual focus on both (1) organizational leaders and (2) IT operations/assurance professionals, both of whom have information assurance concerns. The book offers a range of grounded examples and thought-provoking case discussions with well-framed questions to stimulate critical thought among business leaders and IA professionals. This diversity of reader audiences is a profound strength of this particular work. It is one of these information assurance books that belongs on your professional book-stand, in order to serve as a ready reference for the thoughtful application of information assurance; principles, frameworks and controls to meet our dynamic IT security challenges. The book’s appendices are both rigorous in substance and useful for a review of terms that are in use, in dealing in a present set of common IA threats, supported by a dynamic glossary and electronic citation for further IA references.

Download to continue reading...