INFORMATION ASSURANCE Handbook

Effective Computer Security and Risk Management Strategies

DR. COREY SCHOU & STEVEN HERNANDEZ

Foreword by former U.S. Cybersecurity Coordinator, Howard A. Schmidt

Mc Graw Hill Education

Information Assurance Handbook

Effective Computer Security and Risk Management Strategies

Corey Schou
Steven Hernandez

New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

Cataloging-in-Publication Data is on file with the Library of Congress

Information Assurance Handbook: Effective Computer Security and Risk Management Strategies

1234567890 DOC DOC 10987654

ISBN 978-0-07-182165-0
MHID 0-07-182165-1

Sponsoring Editor
Meghan Riley Manfre

Editorial Supervisor
Patty Mon

Project Manager
Ridhi Mathur,
Cenveo® Publisher Services

Acquisitions Coordinator
Mary Demery

Technical Editors
Flemming Faber
Jill Slay

Copy Editor
Kim Wimpsett

Proofreader
Susie Elkind

Indexer
Rebecca Plunkett

Production Supervisor
Jean Bodeaux

Composition
Cenveo Publisher Services

Illustration
Andrew Berg
Jonathan Holmes
Cenveo Publisher Services

Art Director, Cover
Jeff Weeks

For my family—more patient than I deserve; for my mentors, who gave me the lamp to guide me; for my students, who give me constant purpose and challenge.

—*Corey Schou*

For my beloved wife, Michelle; you inspire the very best in me.

—*Steven Hernandez*

About the Authors

Corey Schou, Ph.D., is a Fulbright Scholar, a frequent public speaker, an active researcher, and an author of more than 300 books, papers, articles, and other presentations. His interests include information assurance, risk management, software engineering, developing secure applications, security and privacy, and collaborative decision making.

He has been described in the press as the father of the knowledge base used worldwide to establish computer security and information assurance. He was responsible for compiling and editing computer security training standards for the U.S. government.

In 2003, he was selected as the first University Professor at Idaho State University. He directs the Informatics Research Institute and the National Information Assurance Training and Education Center. His program was recognized by the U.S. government as a Center of Academic Excellence in Information Assurance and is a leading institution in the CyberCorps/Scholarship for Service program.

In addition to his academic accomplishments, he holds a broad spectrum of certifications including Certified Cyber Forensics Professional (CCFP), Certified Secure Software Lifecycle Professional (CSSLP), HealthCare Information Security and Privacy Practitioner (HCISPP), CISSP Information Systems Security Architecture Professional (CISSP-ISSAP), and CISSP Information Systems Security Management Professional (CISSP-ISSMP).

During his career, he has been recognized by many organizations, including the Federal Information Systems Security Educators Association, which selected him as the 1996 Educator of the Year, and his research and center were cited by the Information Systems Security Association for Outstanding Contributions to the Profession. In 1997, he was given the TechLearn award for contributions to distance education.

He was nominated and selected as an honorary Certified Information Systems Security Professional (CISSP) based on his lifetime achievement. In 2001, the International Information Systems Security Certification Consortium $(ISC)^2$ selected him as the second recipient of the Tipton award for contribution to the information security profession. In 2007, he was recognized as a Fellow of $(ISC)^2$.

Steven Hernandez, MBA, CISSP, CISA, CSSLP, SSCP, CAP, HCISPP, CompTIA Security+, is the chief information security officer for the Office of Inspector General at the U.S. Department of Health and Human Services (HHS). His 16 years of extensive background in information assurance includes work for international heavy manufacturing, large finance organizations, academia, government agencies, nongovernment organizations, and international not-for-profits.

Hernandez is an industry-recognized expert in risk management, information assurance investment performance, privacy in healthcare and commerce, and information assurance management. He guest lectures at Idaho State University as affiliate faculty, the National Information Assurance Training and Education Center as affiliate faculty, George Washington University as a distinguished speaker, and California State University at San Bernardino as an honorary professor. He is the editor and lead author of the third edition of the *Official (ISC)² Guide to the CISSP CBK*. Hernandez is the chair of the (ISC)² HCISPP Common Body of Knowledge Domain committee in addition to editor of the first edition of the Official (ISC)² Guide to the HCISPP CBK.

About the Technical Editors

Flemming Faber is the senior adviser at the Danish Centre for Cyber Security, part of the Danish Defence Intelligence Service. He has been an information security expert since 1994 and was the first Dane to obtain CISSP certification in 1999. Flemming has worked as a security consultant and information security manager in international consultancy companies for a decade. In 2003, he joined the Danish National IT and Telecom Agency, a Danish government agency where he was head of the IT security division until 2009. In the agency, he was in charge of the information security strategy in relation to the general Danish e-government initiatives, the Danish government's information security awareness campaigns, privacy initiatives, and the development of information security standards for Danish government agencies. Since 2006, Flemming has been the Danish government representative on the board of the European Network and Information Security Agency (ENISA). He was the main architect in establishing the Danish GovCERT in 2009, where he is responsible for policy, strategy, and international cooperation. Since 2011, the Danish GovCERT has been part of the Danish Centre for Cyber Security under the Ministry of Defence. He has been active in promoting information security internationally and has been involved with (ISC)² activities since 1999. Flemming was a member of the (ISC)² Board of Directors from 2010 to 2013.

Jill Slay is the director of the new Australian Centre for Cyber Security at UNSW Canberra @ ADFA. With long-term funding allocated, this centre aims to develop critical mass in cross-disciplinary research and teaching in cybersecurity to serve the Australian government and Defence Force and help strengthen the digital economy. She carries out collaborative research in forensic computing, information assurance, and critical infrastructure protection with industry, state, and federal government partners in Australia, South Africa, the United States, and Asia; and she has advised various governments, supporting them in research and process development.

Jill was made a member of the Order of Australia (AM) in the 2011 Australia Day Honours Awards for service to the information technology industry through contributions in the areas of forensic computer science, security, protection of infrastructure, and cyberterrorism. She is a member of the Institute of Electrical and Electronic Engineers and also a fellow of the (ISC)² and the Australian Computer Society. These awards were made for her service to the IT security profession.

Foreword

Throughout my career in government and private industry, I have seen many approaches to securing information systems and managing risks. One question I get asked repeatedly is, "How do I know when I have enough people, process, or technology to manage risk effectively?" In government and regulated sectors, the response to this question is driven by a complex assortment of standards, mandates, and laws pushing to compliance. In private industry, we often see businesses conforming to "best practices" or "industry standards" as a baseline. While conforming to regulatory or legal requirements is a good start, it really is just the bare minimum if an organization wants to excel and mature in risk management. For years I have said, "One can be compliant but still be insecure, and we need to make sure that by being secure we become compliant."

Schou and Hernandez's book provides a leadership view of information assurance and a practical perspective for both practitioners and aspiring leaders. They take the reader through the international dimensions of risk management for strategic leaders and senior management. Their approach not only guides the reader through the necessary elements of managing risk in today's ever-changing IT environment, but also explains why information assurance is important in creating and maintaining a competitive advantage in today's global economy. They give the reader practical advice for approaching information assurance for emerging technologies, such as the cloud and big data, without getting caught up in the technical details that may confuse or distract leadership.

When I served as vice chair of the President's Critical Infrastructure Protection Board and later as the first Cyber-Security Coordinator of the Obama Administration, I worked with Dr. Schou to improve the responsiveness of academia to both government and industry needs. In the preparation of the *U.S. National Strategy to Secure CyberSpace* and subsequently in the *National Strategy for Trusted Identities in Cyberspace*, the essential linkage between strategic leadership and operations was critical. One of the most difficult challenges I faced was conveying risk; good news needs to travel fast, but bad news needs to travel faster. It is critical to pass the bad news on to senior leaders who may not have an extensive background in information technology or security.

This book functions as a bidirectional guide for leadership and operational personnel alike. For those who are more focused on operational and technical issues, the book provides a guide to why senior leaders insist on specific procedures and visibility. For senior leaders, this book provides information about organizational objectives while explaining some of the limitations and capabilities of today's information assurance risk management tools and professionals. The authors offer real-world examples of applying information assurance in industries such as healthcare, retail, and industrial control systems.

This book takes a broad perspective and is a nexus of information assurance practice, policy, strategy, and implementation applicable to a diverse audience. It provides an up-to-date guide covering some of the best information assurance practices found internationally. System administrators can use the book to understand how risk management operates throughout their organization and why their role is significant. Government leaders can gain new insights into cloud computing concerns and how big data integrates with information assurance and risk management. As the authors state in their introduction, "If you need help, read this book!"

—Howard A. Schmidt, Partner, Ridge Schmidt Cyber LLC,
and former Cyber-Security Coordinator of the Obama Administration

Acknowledgments

We would like to thank those who have contributed to the writing and development of this book, including our colleagues and the project team at McGraw-Hill Education, specifically Meghan Manfre, Mary Demery, Patty Mon, and Jean Bodeaux. We would also like to thank Dr. Larry Leibrock for valuable input about computer forensics and Andrew Berg and Jonathan Holmes for the illustrations you will see in the introduction and throughout this book.

Introduction

Information assurance is not my problem, and it is not your problem. It is an ever-increasing problem for *everyone*—you, home businesses, small enterprises, large businesses, economies, and governments are all at risk. Think of it this way: Information and data in all forms are assets, and you are obliged to protect your assets. Of course, as you run your enterprise, your security efforts do not show up on the bottom line—unless something goes wrong. All information assurance tools and mechanisms required by the largest enterprises are useful at a different scale by the smallest. This book allows you to select from a broad spectrum of information assurance tools to protect assets, manage risk, and provide competitive advantage. While reading, you will see the "juggling leader" as a callout for concepts that warrant special attention for those wearing many hats. She will point out useful subject matter for people juggling several roles.

Read This Book

If you run a one-person enterprise, you must perform a constant balancing act or become a one-man band and keep your focus on the overall success of the enterprise. At a minimum, you must have a plan for what you would do if something destroyed all your records or if a virus took over your computers or if a competitor took your list of prospects or...well, you get the idea. Information assurance must be part of your enterprise planning. You must make yourself do information assurance if you are to remain viable and competitive!

Read This Book

If you run a small to medium enterprise, you may be able to have some specialization among your employees. This is like having a low-budget jazzband or a classic ensemble where the musicians all wait tables in a restaurant on the side (using the same tux for both jobs). If you are lucky, you might have someone who is in charge of information technology. This individual must devote part of their time to information assurance and may provide some leadership, but they also have to support employees and customers. They have help, but you must provide direction and leadership. For example, your accounting staff, your marketing staff, and your production staff will have a role in information assurance, but they must all be going in the same direction. Remember, they will all plead that information assurance is not their job. You as a leader must set the example and the tone from the top. Information assurance must be part of your enterprise planning. You must provide leadership and encourage an information assurance culture. How?

Read This Book

If you run a large enterprise, you have all the challenges of protecting your information assets through a CIO. While the CIO may have good intentions, understanding information assurance and being able to *speak* its language is invaluable when explaining problems, opportunities, and risk to technical professionals. Information assurance must be part of your enterprise planning. It must be central to your information technology strategy. You must provide leadership and encourage an

information assurance culture. In today's competitive and global marketplace, even large enterprises that have existed for years without a formal information assurance function can stumble and fail rapidly because of a breach or cyberattack.

Consider information assurance as a professional symphony orchestra: It has all the attributes of an ensemble and a one-man band. Each group can select more or less complex versions of the music just as you can choose lessons from this book. Take what you need, but read through the book from time to time to see what you might be missing. No matter what, have a plan, execute it, mitigate risk, succeed. Half the battle is choosing the right questions to ask at the right time! This book aims to arm the senior leaders of the organization with the strategic tools to help have constructive discussions around information risk, assurance, and strategy. The conductor of an orchestra doesn't need to understand how to play every instrument. However, she must understand the basic sounds, notes, combinations, and types of music best performed by specific instruments. It is essential that all of this is done in perfect harmony.

This book takes a similar approach with information assurance. Reading it will not make a senior leader a *cyberninja* with deep technical skills. It will, however, create a leader with a strong information assurance strategic understanding who can call in the right combination of skills, experience, and background to meet today's toughest risk management challenges. Remember, the Spartans were amazing soldiers and well-trained in a narrow field. They had numerous amazing battles we remember today; ultimately, though, they were defeated by forces that understood not only warfare but how to mix strategic resources to mitigate risk and deliver results! If you are already experienced with the technology portion of the information assurance profession, reading this book will help you understand what your senior management is trying to do through their strategic planning.

Purpose

Enterprises of all sizes are under increasing competitive pressure to leverage data, information, and communication technology infrastructure to achieve their vision. The well-planned implementation of secure information technology will have a large positive impact on the socio-economic development of an organization and its partners. While information technology (IT) clearly revolutionizes businesses and strengthens governments, it introduces risks.

To make the IT investment pay off, senior management must address and manage risks systematically and economically. Assuring the information assets have integrity, are available, and are confidential presents a significant challenge to even seasoned executives; improvement in this area is a continuous effort. The strategic approach and controls explained provide an executive view of information assurance. The controls and strategic approach are also expected to guide an overall strategy for safeguarding vital information assets and critical functions of an organization.

The essentials of information assurance have been identified and mapped for the senior management and executives of an organization. Our approach to information assurance is broad to ensure that the contents are relevant to organizations of various sizes, complexities, and industries. Assuring information and providing security is an

ongoing process; an organization's information assurance policy is an instantiation of a living organizational strategy and helps management establish an organization's risk management strategy.

We have provided best practices and guidelines to assist in preventing, detecting, containing, correcting, and recovering from inevitable security breaches and other information assurance failures. By providing a broad overview of threats, information assurance concepts, and risk management approaches, organizations may use the information presented to strengthen their information assurance risk posture. An organization's mission and objectives are always put first if information assurance is pervasive and not invasive in the organizational culture.

The information presented is designed to reach a broad audience; the content does not provide detailed implementation procedures for security controls nor does it prescribe minimum compliance requirements or penalties for noncompliance. Guidance is provided to management to seek an in-depth solution for their particular challenges. Organizations should seek professional opinions from appropriately certified professionals before implementing security controls that are in accordance with their risk profiles and business objectives.

No matter the size of your enterprise, investing in information assurance controls requires a commitment of limited finances, time, and human resources. It may not be feasible for organizations to invest in all areas of information assurance. The information provided is intended to foster discussion around possible approaches and help organizations prioritize areas for improvement.

The information assurance strategic approach and associated controls provide fundamental information and guidelines for senior management and executives of organizations. The approach outlined provides guidance for protecting information system–based assets (including information, software, and hardware) by describing the interrelationships and provides a comparison analysis of information assurance elements. Executives and senior management who need quick and broad overviews on information assurance–related matters will find this resource useful.

Scope

The material presented is useful to organizations independent of the following:

- Nature of business (telecommunication, education, utility, health, defense)
- Size (small, medium, large)
- Type (commercial, government agencies, nonprofit)

Guidelines are provided for managing information assurance, and we demonstrate a comprehensive approach to identifying, applying, and controlling information assurance initiatives. Common threats and vulnerabilities are discussed as you are guided through a comprehensive list of applicable controls for an organization as a function of its risk profiles.

The approach offered does not go in-depth into implementation procedures. Organizations should view the strategy and controls offered as advisory and use the

contents as a starting point to manage its assurance exposures. The strategy and controls are vendor-independent and are not specific to any technology. Every section includes critical thinking questions. These questions are intended to guide you in applying the material discussed to their organization or mission.

Intended Audience

The strategy presented provides a foundation for a broad audience—experienced and inexperienced, technical and nontechnical—who invest in, monitor, administer, support, manage, audit, assess, design, and implement information assurance within their enterprise. These personnel include the following:

- Anyone within an enterprise who wants to know more about information assurance and who is responsible for planning, managing, implementing, operating, and improving the information assurance management system
- Anyone who wants to be able to identify and manage risk
- Business owners and mission owners who rely on information systems but may not have a good understanding of IT risk and how to manage it
- Chief information officer (CIO), who ensures the implementation of information assurance for an organization's information systems
- Chief risk officer (CRO), who needs to be able to identify and manage enterprise risk
- Contract officers, program managers, and acquisition professionals who are responsible for the IT procurement process
- Enterprise owners ranging from single proprietors to small and medium businesses who want to protect their assets and manage risk
- Information assurance program manager or chief security officer (CSO) and the chief information security officer (CISO), who implement the security program
- IT auditors who audit the systems and ensure compliance with the relevant policies and regulations
- New employees who want to understand why their organization has so many rules, policies, and guidelines
- Senior management, executives, or business owners, who plan and approve budget and set business strategy and objectives
- System and information owners, who are entrusted to protect information and information systems in accordance with the protection requirements stipulated
- Technical support personnel (such as application, system, network, and database administrators), who manage and administer security for the information systems
- Anyone who must balance information assurance and their primary job responsibilities

Throughout the book, there are opportunities for you to challenge yourself with critical thinking exercises. The answers to these questions are not right or wrong; they are intended to stimulate your thinking about information assurance. Responses for each question are included in the appendix section of the book.

William Shakespeare told us that "one man in his time plays many parts" and so it is in information assurance. The list of roles appears daunting; however, no matter the size of the organization, someone has to perform the roles.

Overview

We have organized the contents into six parts. Each of these parts is divided into several chapters focused on essentials. Since each chapter is designed to be self-standing, each chapter has a set of critical thinking exercises for self-assessment and a selection of further readings. In general, this structure models an organizational strategy for information assurance (see Figure 1).

Part I: Information Assurance Basics

Part I introduces the essential-to-know matters in information assurance including the need for information assurance, popular concepts, and approaches. Relationships among fundamentals such as assets, threats, vulnerabilities, risks, and controls are discussed. Since there are several interpretations of the terms *information assurance*, *information security*, and *cybersecurity*, we have developed a model showing the relationship among them. Different types of security professionals and professional organizations will also be discussed. It is important to understand the information assurance management system (IAMS) and how information assurance is a continuous process. This part ends with a discussion of current practices and regulations in the existing competitive market and information technology landscape.

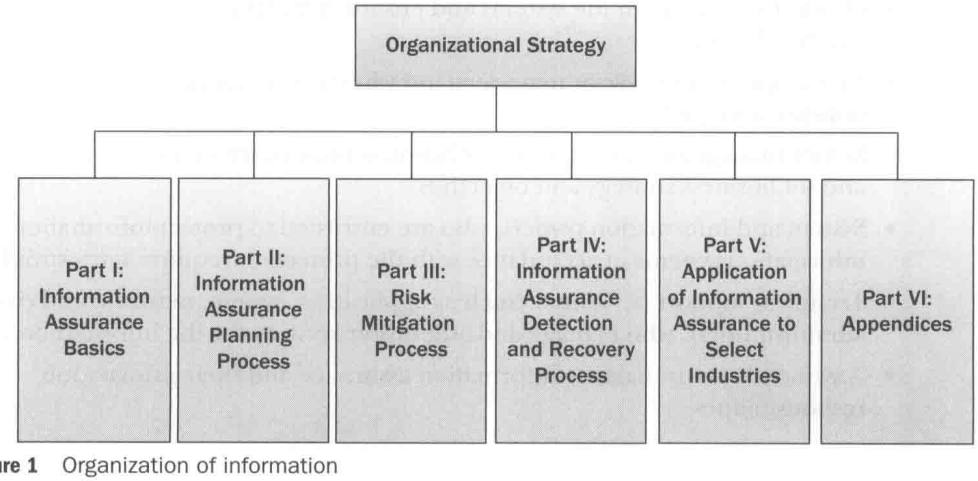

Figure 1 Organization of information