Computer Communications and Networks

Springer-Verlag London Ltd.

The **Computer Communications and Networks** series is a range of textbooks, monographs and handbooks. It sets out to provide students, researchers and non-specialists alike with a sure grounding in current knowledge, together with comprehensible access to the latest developments in computer communications and networking.

Emphasis is placed on clear and explanatory styles that support a tutorial approach, so that even the most complex of topics is presented in a lucid and intelligible manner.

Also in this series:

An Information Security Handbook
John M.D. Hunter
1-85233-180-1

Multimedia Internet Broadcasting: Quality, Technology and Interface
Andy Sloane and Dave Lawrence (Eds)
1-85233-283-2

The Quintessential PIC Microcontroller
Sid Katzen
1-85233-309-X

Andrew Blyth and Gerald L. Kovacich

Information Assurance

Surviving in the Information Environment

Springer

Andrew Blyth, PhD, MSc
School of Computing, University of Glamorgan, Pontypridd,
Mid Glamorgan CF37 1DL, UK

Gerald L. Kovacich, D.Crim, MSc, MA
ShockwaveWriters.com, Whidbey Island, WA, USA

Series editor
Professor A.J. Sammes, BSc, MPhil, PhD, FBCS, CEng
CISM Group, Cranfield University, RMCS, Shrivenham, Swindon SN6 8LA, UK

British Library Cataloguing in Publication Data
Blyth, Andrew
Information assurance : surviving in the information
environment. - (Computer communications and networks)
1. Data protection
I. Title II. Kovacich, Gerald L.
005.8

Library of Congress Cataloging-in-Publication Data
Blyth, Andrew, 1966-
Information assurance : surviving in the information environment. / Andrew Blyth and
Gerald L. Kovacich.
p. cm. -- (Computer communications and networks)
Includes bibliographical references and index.

1 Computer security. 2. Data protection. I. Kovacich, Gerald L. II. Title. III. Series.
QA76.9.A25 B59 2001
005.8—dc21

2001032780

Computer Communications and Networks ISSN 1617-7975

ISBN 978-1-85233-326-3 ISBN 978-1-4471-3706-1 (eBook)
DOI 10.1007/978-1-4471-3706-1

http://www.springer.co.uk

Originally published by Springer-Verlag London Limited in 2001.

Typesetting: Camera-ready by authors

34/3830-543210 Printed on acid-free paper SPIN 10768781

Dedications

To my Wife, who is always there when I need her the most and without whose love and support, I would not have been able to complete this book.

Dr. Andrew J. C. Blyth
University of Glamorgan
United Kingdom

This book is dedicated to all those professionals in the world's government agencies and businesses who are responsible for providing leadership for the protection, integrity and availability of the sensitive information on which we all depend.

Dr. Gerald L. Kovacich, CFE, CPP, CISSP,
Whidbey Island, Washington
United States of America

Quotations

"Our wish... is that... equality of rights [be] maintained, and that state of property, equal or unequal, which results to every man from his own industry or that of his fathers." --Thomas Jefferson: 2nd Inaugural Address, 1805.

"To take from one because it is thought that his own industry and that of his father's has acquired too much, in order to spare to others, who, or whose fathers have not exercised equal industry and skill, is to violate arbitrarily the first principle of association—'the guarantee to every one of a free exercise of his industry and the fruits acquired by it.'" --Thomas Jefferson: Note in Destutt de Tracy's "Political Economy," 1816.

Foreword

When you first hear the term Information Assurance you tend to conjure up an image of a balanced set of reasonable measures that have been taken to protect the information after an assessment has been made of risks that are posed to it. In truth this is the Holy Grail that all organisations that value their information should strive to achieve, but which few even understand.

Information Assurance is a term that has recently come into common use. When talking with old timers in IT (or at least those that are over 35 years old), you will hear them talking about information security, a term that has survived since the birth of the computer. In the more recent past, the term Information Warfare was coined to describe the measures that need to be taken to defend and attack information. This term, however, has military connotations - after all, warfare is normally their domain. Shortly after the term came into regular use, it was applied to a variety of situations encapsulated by Winn Schwartau as the three classes of Information Warfare:

Class 1 - Personal Information Warfare.
Class 2 - Corporate Information Warfare.
Class 3 - Global Information Warfare.

Political sensitivities lead to "warfare" being replaced by "operations", a much more "politically correct" word. Unfortunately, "operations" also has an offensive connotation and is still the terminology of the military and governments. A term was needed that described the measures needed to safeguard the most precious asset in this modern, connected world - Information. The measures are much more than just security, encompassing the concepts of risk assessment, management and the protection of your information from compromise, theft, modification and lack of availability.

Information Assurance is ensuring that your information is where you want it, when you want it, in the condition that you need it and available to those that you want to have access to it - but only to them. In the past, information was recorded, stored and transported on paper, the methods of achieving security were developed over more than three thousand years, and had the distinct advantage that any action that was taken on the information could normally be easily observed. Now and increasingly in the future, information exists digitally and digital technology has only been in common use for less than 30 years. Add this shortage of time in which to gain experience in the best methods of protecting digital information to the fact that it can be moved from one place to another in a fraction of a second. Then add the facts that it can be stolen and yet remain unaffected in its original location; that vast quantities of it can be stored on increasingly small storage mediums and that you can no longer easily view, even with equipment to assist you, what is contained on the storage medium; and you begin to comprehend the problems of Information Assurance.

Modern day security specialists have an increasingly difficult problem to solve. In addition to the aforementioned factors, the technologies (both in hardware and software) are changing with increasing rapidity, making it even more difficult for even the most dedicated of professionals to gain and maintain the knowledge needed to allow them to effectively carry out their tasks.

The problem is compounded by the way in which we as a society organise ourselves. People who are involved in Information Assurance are mostly employed in the business of security and use the skills and knowledge that they have obtained to stop unauthorised users from gaining access to the information. As a result of this, they will tend not to share the information and knowledge that they have collected in order to protect the methods that have been used to acquire it. They will also tend not to advertise that they have suffered an attack to avoid embarrassment to their organisation and limit the damage that such an attack has caused. Those who attack information systems gain their knowledge by sharing and communicating with others of a similar persuasion in a culture of peer recognition and a shared goal.

We are all striving for a globally connected society where everyone is encouraged to make use of the information systems that are available, and those that cannot are considered to be disadvantaged. It is not surprising in this environment that we are seeing a growth in the level of a whole range of crimes that were previously seen in the paper based society migrating to this new medium. We have made it possible for a person who would wish to harm our interests to gain the three elements that they seek most – access to our valuables, the opportunity to remain anonymous and the potential to carry out the attack without having to physically visit the site of the attack – indeed, it is not even necessary to visit the country in which the attack is mounted.

Given that the problem is, in historical terms, very new and also global, it is not surprising that national legal systems are having difficulty in addressing the problem and that the international community, not renowned for its speed, is talking about the problem but not yet acting in response to it.

In the coming months and years, we will witness technological solutions to Information Assurance needs and comparisons will be seen with the way in which we handle the physical valuables of today. Strong-rooms that protect the physical environment will be matched by secured data warehouses and protected servers, couriers by encryption and digital signatures, locks on the doors by firewalls and security alarms and burglar alarms by Intruder Detection Systems in the virtual world. What of keys, oh yes, biometric devices and smart cards - whatever next?

Andy Jones MBE BSc MBCS
Group Manager, Secure Information Systems; Defence Evaluation and Research Agency (UK)

Preface

In the late 1970s and early 1980s, information systems security began to gain in importance as more and more government agencies and businesses began to integrate computers into their processes. The 1990s was the decade of the massive integration of computers into corporate, national and international networks. The Internet became the backbone for the global networking of networks.

The information systems security profession was born and began to mature during this time. The concept of protecting computer systems and by doing so also protecting the information they processed, stored and transmitted was the norm. However, gradually another concept began to take hold, and that is the concept of information assurances (IA). IA is more than just information systems security or information security. The development of the concept of IAs is another step in the maturation of concepts, practices and processes needed to protect information, the vital asset of today's information-based, information-dependent nation-states and corporations.

As the threats, internal, national, and global to information grows, so is the need to develop new, more sophisticated holistic IA processes. However, before that can be accomplished successfully, one must understand the concept of IAs and surviving in the information environment. It is hoped that this book will assist in meeting those challenges.

This book aims to perform two very important functions:

- To bridge the gap between information assurance as a technical concept and IA as a business concept. Thus allowing information systems managers to effectively manage information systems' security in such a manner so as to facilitate the business process and contribute to the competitive advantage of the organisation.
- To provide information systems managers and students with a core text on assuring accurate information is available when needed to only those that need it. As the Internet continues to expand and more companies start conducting business on the Internet, electronic business, there is going to be a need for people who understand not only the IA concepts and best practices, but also the business, legal and technical aspects of conducting business online. It is hoped that this book provides some assistance in that endeavour.

The book is divided into four sections and a total of fifteen chapters as follows:

Section 1 – An Introduction to Information Assurance

This section sets the context of the book, and talks about the need for all organisations to take IA seriously. It will also provide an introduction to IA and related topics. It will provide the reader with a baseline on which to build an understanding of the theories, philosophies, models, processes, management, and technical aspects of IA.

Chapter 1. What is Information Assurance?
This chapter will define basic terms such as IA, information operations, information security, information systems security, and information warfare. It will also provide a short history of these concepts.

Chapter 2. The World of Information
This chapter will discuss the global and national economic and political environment as it relates to conducting business and the increasing need for IA in this new global marketplace.

Chapter 3. The Theory of Risks
This chapter will define and discuss threats, vulnerabilities, and risks. Also addressed will be the concepts of qualitative and quantitative risk analysis and risk management vis-à-vis IA.

Chapter 4. The Information World of Crime
IA is required because of human error and because there are people in business and throughout the world who will use any legal and illegal means in order to obtain information for resale or to give others a competitive advantage. These issues will be discussed in this chapter based on theories of criminology, psychological profiling, and examples of actual cases will be analysed. Included will be a discussion of inquiries, investigations and examinations of incidents caused by these miscreants, to include a discussion of computer forensics. Included will be an introduction to cybercrime and the effect that it can have on organisations and businesses, e.g. public confidence in CITI-Bank.

Chapter 5. IA Trust and Supply Chains
In this chapter, the idea of trust within organisations, processes, and systems will be discussed along with the idea of supply chains.

Chapter 6. Basic IA Concepts and Models
Building on the above, this chapter will address the various IA related models such as: The Confidentiality-Integrity-Availability (CIA) Model; The Protect-Detect-React-Deter (PDRD) Model; The Need-to-Know (NTK) Model; and The Information Value (IV) Model.

Section 2 – IA in the World of Corporations

This section will begin with a discussion of the corporate security officer, to include a description and discussion of their duties and responsibilities, and their IA role. This will be followed by a discussion of the corporate IA officer, and the functions of an IA organisation within a corporation.

Chapter 7. The Corporate Security Officer
This chapter will identify and discuss the duties and responsibilities of a corporate security officer as it relates to IA and the protection of the corporate assets to include the protection of information and information systems.

Chapter 8. Corporate Security Functions
This chapter will identify and describe security functions of a corporation to include those functions that are an integral part of any corporation's IA program.

Chapter 9. IA in the Interest of National Security
This chapter will describe and discuss IA requirements in the national security environment of government agencies and defence-related businesses since many of the philosophies and processes can be adapted to meet the IA needs of corporations.

Chapter 10. The Corporate IA Officer
This chapter addresses the position of the corporate IA officer. It describes the basic qualifications, duties and responsibilities required to lead an IA effort for a corporation into the 21st century.

Chapter 11. IA Organisational Functions
This chapter will identify and discuss a corporation's IA organisational structure and its IA functions.

Section 3 – Technical Aspects of IA

This section will discuss the technical aspects of IA as it relates to the storing, processing and transmitting of information.

Chapter 12. IA and Software
This chapter will discuss the problems and possible solutions to the IA questions in the software and firmware environment of operating systems, databases, and applications software. Included will be a discussion of malicious codes.

Chapter 13. Applying Cryptography to IA
This chapter will describe and discuss cryptography including when to use it, when not to use it, and the related political ramifications of cryptography in the global marketplace. Topics discussed include algorithms; public and private key; key management; digital signatures; and the world of PKI.

Chapter 14. IA Technology Security
This chapter will discuss the technical equipment available and in use to protect or attack the IA processes including ADT, CCTV, biometrics, EMP weapons, HERF guns, TEMPEST, line filtering, and smart cards.

Section 4 – The Future and Final Comments

This section will provide the authors' final comments, predictions and conclusions.

Chapter 15. The Future, Conclusions and Comments
This chapter will summarise the main points of the book, draw some conclusions, and look into the future of IA as we enter the 21st century.

Acknowledgements

To successfully take on and complete such a project as writing this book, one must rely on many people who freely give of their professional advice and assistance. We are grateful to the following friends and colleagues for their never-ending support and consultations: Andy Jones, William C. Boni, Perry G. Luzwick, Paul Zavidniak, Ed Halibozek, and Motomu Akashi.

A special thanks to John Meyer, Reed Elsevier's Advanced Technology Group, Oxford, England; and to Carola E. Roeder, Permissions, Butterworth-Heinemann, a member of the Reed Elsevier Group, Woburn, Massachusetts, USA; for their years of support and for granting permission to include relevant material from Dr. Kovacich's other books and articles published by them. Also to Ken Cutler, CISA, CISSP, Managing Director, Information Security Institute, for providing the "MIS Training Institute Swiss Army Knife"; and Keith Lawrence Buzzard, B.Sc, M.Sc., for a copy of his paper, "Computer Misuse Act 1990 - Loopholes and Anomalies".

Regardless of how much good advice we received from our colleagues, this book could never have been successfully published if it were not for Rosie Kemp of Springer-Verlag, our publisher, who was willing to risk signing a couple of "crazy doctors" to a book contract. Thanks Rosie!

Writing and publishing this book was truly a team effort. Other members of that team who made this all possible deserve a note of appreciation. They are: Karen Borthwick, Sally Tickner, and Joanne Cooling.

Contents