Guarding Your Business

A Management Approach to Security

Guarding Your Business

A Management Approach to Security

Edited by

Sumit Ghosh
Manu Malek

and

Edward A. Stohr
Stevens Institute of Technology
Hoboken, New Jersey

KLUWER ACADEMIC PUBLISHERS

NEW YORK, BOSTON, DORDRECHT, LONDON, MOSCOW

eBook ISBN: 0-306-48638-5
Print ISBN: 0-306-48494-3

©2004 Kluwer Academic Publishers
New York, Boston, Dordrecht, London, Moscow

Print ©2004 Kluwer Academic/Plenum Publishers
New York

All rights reserved

No part of this eBook may be reproduced or transmitted in any form or by any means, electronic, mechanical, recording, or otherwise, without written consent from the Publisher

Created in the United States of America

Visit Kluwer Online at: <http://kluweronline.com>
and Kluwer's eBookstore at: <http://ebooks.kluweronline.com>

PREFACE

INTRODUCTION

The industrial landscape of yesterday was a collage of companies with diverse products and resources, the only common element between them being people. Today, and increasingly in the future, virtually all organizations will feature computing and intelligent networking infrastructure as a common and one of the most important resource. This is not entirely surprising since computers represent an extension of the human mind while networked systems reflect the essential architecture of human civilization. The result has been mixed. While the industries' reach now extends far and wide, a new kind of threat looms on the horizon. Loosely encompassed by the terms cyber-threat and cyber-crimes, these threats are extremely powerful, occur rapidly, and are often subtle and elusive.

In the last two decades, increasingly banks and financial institutions have been conducting transactions over the Internet using different geographically dispersed computer systems. Today, businesses that accept transactions via the Internet gain a competitive edge by reaching a worldwide audience at relatively low cost. The Internet, however, poses a unique set of security issues that businesses must address at the outset to minimize risk. Customers will submit information via the Web only if they are confident that their personal information, such as credit card numbers, financial data, or medical history, is secure. As we are continuing to learn, security is not always a given and, most important, it is not absolute. For example, in July 2001 Microsoft conceded that all versions of Windows 2000 and early "beta" versions of its new XP operating system contained a "serious vulnerability" that allows hackers

to take control of victims' machines. Microsoft promised to cure the problem before XP's rollout. But reportedly, after a few hours of the announcement of Windows XP on October 10, 2001, it was hacked! The threats, risks, and failures in the computing and networking world mirror those in the physical world, but the risk factors in the electronic world are different. Failures are more widespread; failures stemming from attacks are harder to predict; and the effects of attacks are devastating. Paper data, even where public, is hard to search and correlate. In contrast, electronic data can be searched easily and networked data can be searched remotely and correlated with other databases.

A 1996 GAO report estimated that 250,000 attacks per year had been perpetrated against the Department of Defense computer systems, and that the rate of attack was increasing by about 100% per year. According to the FedCIRC, the incident handling entity for the federal government, 130,000 government sites totaling more than one million hosts were attacked in 1998. Also, a 2002 survey conducted by the Computer Security Institute and the FBI revealed that 90% of the 507 participating organizations detected computer security breaches within the past 12 months, 74% cited their Internet connections as a frequent point of attack, but only 34% reported the intrusions to law enforcement. These numbers must be taken with a big grain of salt since they only relate to known attacks and vulnerabilities.

A key to preventing security attacks is to understand and identify the IT infrastructure vulnerabilities, and to take corrective action. Where corrective action is difficult, attacks must be monitored to estimate the time and extent of penetration by perpetrators. Also the value of information to an organization must be estimated. Businesses create and collect a tremendous amount of information, such as employee information, customer information, product information, and process information. Such information is widely distributed due to increasing employee mobility, companies migrating from a centralized to a distributed computing environment, companies growing their reach geographically, and as a result of employee mobility. Information is a major business asset: the nature and quality of information, and how effectively it is used, distinguishes an organization from its competitor.

OBJECTIVE OF THE BOOK

This book encapsulates the proceedings of the Management of Technology (MOT) Symposium held at Stevens Institute of Technology during October 22–24, 2002 and is the first in a planned series of books that will accompany Stevens' MOT Symposium Series (<http://attila.stevens-tech.edu/motsymposium>).

The title of the book reflects the symposium's focus in 2002, namely, security (the issues that managers must address to safeguard their organizations against potentially devastating electronic attacks) architecture for business. Subsequent symposia will cover other topics within the broad framework of technology management.

The objective of this book is to provide business managers a complete and comprehensive awareness of basic network security issues at the correct level of detail so they can make decisions that are sound from both scientific and business perspectives. Subsequent symposia will cover other topics within the broad framework of technology management, grounded in science and engineering. Selected symposium speakers and other experts were invited to write the chapters for this volume in their specific areas of expertise and were requested to add case studies to strengthen coverage of the issues.

OVERVIEW

This book outlines the organizational elements that must be in place to protect the information assets of the organization. These elements include technologies such as encryption, firewalls, biometric devices, and back-up and recovery mechanisms. All of these technical elements must be employed within a comprehensive framework of architecture so as to systematically guard against hostile intrusion, resist human error, and survive physical attack and natural disaster. Attributes of the architectural framework include risk assessment, determination of quality-of-service levels that balance safety versus cost, disaster recovery procedures, determination of access rights to data and software, and a security-conscious culture in the organization. Thus, the main message of the book is that the architecture must parallel the physical structure of the organization that has long been designed to

systematically protect the physical assets of the organization. Questions answered by the book include: How can one organize for security? What are the fundamental issues in network security? What organizational structures, policies, and procedures must be in place? What legal and privacy issues must be addressed?

ORGANIZATION OF THE BOOK

The book is divided into four parts, Part I through Part IV. Part I presents background information through two chapters. Chapter 1 includes an overview of the security threats and techniques and explains authentication, encryption, and public-private key mechanisms in detail. Chapter 2 examines the nature of network security from a fundamental perspective and develops a systematic logical analysis to present a clear picture of the past and a glimpse of the future.

Part II addresses security threats to organizations in three chapters. Chapter 3 enumerates the actual experiences of the Commanding Officer of the Computer Crimes Investigation Unit of the New York Police. This eye-opening chapter reveals how quickly most passwords may be cracked automatically, even those borrowed from dictionaries in foreign languages, and how perpetrators may leave silent background scripts running on computers to capture every keystroke of an unsuspecting user. Chapter 4 describes the results of a war-gaming exercise involving cyber-attacks on the nation's networking infrastructure including telecommunications, Internet, electric grid, and financial services. Chapter 5 explains U.S. laws that are designed to fight security threats and expresses justifiable concern that laws recently passed by U.S. Congress in the wake of the 9/11 incident may seriously undermine U.S. Citizens' right to privacy as guaranteed by the U.S. Constitution and the Bill of Rights.

Part III reports on the state-of-the-art in security technologies and includes three chapters. Chapter 6 focuses on the specific security needs of the financial industry including protecting information, defeating denial of service, and preventing fraud and identity theft. Chapter 7 reviews the current state-of-the-art in wireless wide-area, local-area, and personal-area networks. Chapter 8 explains the difficulties and

tradeoffs underlying the use of passwords, biometrics, and other methods of authenticating human users.

Part IV describes new methodologies to organize and manage security and comprises three chapters. Chapter 9 discusses the different dimensions of risk management while Chapter 10 is critical of the current security policy that is administered on a piece-meal ad hoc basis. Consequently, different components of network security do not work with one another. The chapter describes the experience with developing and evaluating a smart firewall project. Chapter 11 describes actual experiences related to identifying and closing key security gaps in the Internal Revenue Service's operations. Finally, Chapter 12 reviews in detail the different processes and procedures needed to maintain security in an organization. In essence, it describes the organizational architecture that needs to be in place to guard your business against the many security threats outlined in earlier chapters of the book.

Sumit Ghosh, Manu Malek, and Edward A. Stohr
Stevens Institute of Technology

ACKNOWLEDGMENTS

The editors express their sincere gratitude to all the speakers, contributing authors, and attendees of the 2002 MOT symposium, whose enthusiasm made the symposium a success. Special thanks are due to the organizing committee at Stevens Institute of Technology including Chris Bullen, John Byrne, Stan Clark, Audrey Curtis, Hosein Fallah, Sharen Glennon, Jerry Hultin, John Keating, Rajkumar Kempaiah, Louis Laucirica, B.J. Taylor, Melissa Vinch, and Elizabeth Watson. External advisory board members who deserve our thanks are: Ed Amoroso (AT&T), Ed Cannon (Grey Global), David Luce (Rockefeller Group Inc.) and Daniel Schutzer (Citigroup). Ramaswamy Iyer provided invaluable services in editing and compiling the book. Ana Bozicevic of the editorial department and the production staff at Kluwer Academic/Plenum Publishers deserves our sincerest appreciation.

CONTENTS

PART I: Background

1. Security Principles for Managers	1
Manu Malek	
2. The Fundamental Nature of Network Security	15
Sumit Ghosh	

PART II: Security Threats to the Organization

3. Computer Security: Sophisticated Enemies	33
Yalkin Demirkaya	
4. Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack	47
Eric Purchase and French Caldwell	
5. Cybercrime and the Law: Balancing Privacy against the Need for Security	65
Susan W. Brenner	

PART III: Overview of Latest Security Technologies

6. Some Security Issues and Concerns in the Financial Services Industry	85
Dan Schutzer	
7. Security and Insecurity of Wireless Networks	101
R. Chandramouli	

8. Securing Business’s Front Door: Password, Token, and Biometric Authentication..... 119
Lawrence O’Gorman

PART IV: Organizing for Security–Managerial Issues

9. Managing Information Security Risks across the Enterprise 151
Audrey Dorofee

10. Automatic Security Policy Management in Modern Networks: A New Approach to Security 173
S. Raj Rajagopalan

11. The Internal Revenue Service’s Mission Assurance Program 189
Len Baptiste

12. Organizing for Security 201
Paul Rohmeyer

About the Editors 239

Index 241