Digital Business Security Development:
Management Technologies

Don Kerr, *University of the Sunshine Coast, Australia*

John G. Gammack, *Griffith University, Australia*

Kay Bryant, *Griffith University, Australia*

BUSINESS SCIENCE Reference

BUSINESS SCIENCE REFERENCE

Hershey · New York

Director of Editorial Content:	Kristin Klinger
Director of Book Publications:	Julia Mosemann
Acquisitions Editor:	Lindsay Johnston
Development Editor:	Julia Mosemann
Publishing Assistant:	Travis Gundrum; Jamie Snavely
Typesetter:	Keith Glazewski; Travis Gundrum
Production Editor:	Jamie Snavely
Cover Design:	Lisa Tosheff
Printed at:	Lightning Source

Published in the United States of America by
Business Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Digital business security development : management technologies / Don Kerr, John G. Gammack, and Kay Bryant, editors.
p. cm.
Includes bibliographical references and index. Summary: "This book provides comprehensive coverage of issues associated with maintaining business protection in digital environments, containing base level knowledge for managers who are not specialists in the field as well as advanced undergraduate and postgraduate students undertaking research and further study"--Provided by publisher. ISBN 978-1-60566-806-2 (hardcover) -- ISBN 978-1-60566-807-9 (ebook)
1. Electronic commerce--Security measures. 2. Business enterprises--Computer networks--Security measures. 3. Computer security. I. Kerr, Don, 1952- II. Gammack, John G. III. Bryant, Kay, 1954- IV. Title.

HF5548.32.D538 2010
658.4'78--dc22

2010024585

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Editorial Advisory Board

Table of Contents

Preface

INTRODUCTION

There is a widespread perception that conducting business on the Internet has a higher risk than in the traditional face-to-face environment. This is due, in part, to security concerns and to the need for an extra level of trust incurred when paying for goods or services before receiving them. For the majority of consumers, the benefits of immediate access and search capabilities, as well as 24-hour access to businesses on a global scale, outweigh many of these security and trust concerns. Nonetheless, a healthy skepticism of some Web sites, and to deals offered, is essential because for a few people the Internet provides an easy means of concealing illegal and malicious activities.

While there is a common perception that the security of Internet-based transactions is weak, the reality is otherwise. Current security techniques are much stronger than techniques used when conducting transactions via fax or over the telephone. Nonetheless, although the perception of vulnerability is stronger than the reality, digital threats do need to be taken seriously. If an Internet organization is to survive and prosper, it must be fully aware of the threats and attacks (both internal and external) that can be used against it. Both businesses and government agencies operating electronically need to be vigilant against information theft, espionage and liability. They need to establish as many deterrents, defenses, and security measures as necessary, to protect their systems and data, and to understand the principles behind these to counter new threats. Further, the digital business needs to establish an ongoing maintenance program, and good administrative practices, to ensure security measures are kept up to date.

THE OVERALL OBJECTIVES OF THE BOOK

The overriding aim of this collection is to provide managers with an awareness of a range of issues associated with managing and securing the digital business. The specific objectives of the book are to:

- Provide knowledge on the extent of the security threat for Internet organizations
- Build knowledge about the types of threats facing businesses operating in a digital environment and the solutions that will minimize or eliminate those threats
- Identify common mistakes that businesses make in implementing and managing security
- Develop an appreciation of the importance of management strategies and legislation covering security issues in the digital environment.

THE TARGET AUDIENCE

This book contains state of the art research relevant to informing business practice. It provides base level knowledge for business managers who are not specialists in the field; however, the main audience will be advanced undergraduate and postgraduate students undertaking research and further study in the field, or looking towards a specialised career in this area. By providing an overview of the issues, coupled with in-depth chapters on specific key topics, both breadth and depth are addressed for these readerships. We adopt a managerial, rather than a technical focus, since security principles are more enduring than specific technologies.

BOOK CONTENT

The book emphasizes managerial aspects of security and includes the following chapters:

Chapter 1 is an overview of the digital landscape and specifically looks at digital business security issues. It attempts to cover the areas of most concern, according to contemporary interviews conducted with Information Technology (IT) managers from both government and non-government sources. The issues extracted from these interviews are used to illustrate the major points of concern and the interviewees were chosen to represent real decision makers around security issues.

Chapter 2 considers evidence in forensic investigations. This is an important area because, increasingly, managers are being called on to undertake some form of investigative work due to legal disputes, and breaches of personnel regulations or criminal activity. The chapter presents a review of digital evidence to help business managers gain a practical understanding of digital evidence, and to help them to manage this aspect.

Chapter 3 looks at developments in simplified sign-on authentication. Authentication is the process of determining whether a user is whom they claim to be. This is generally done via a login system, consisting of a user ID and password. As users today have a need for multiple sign-on, this chapter discusses the problem of managing usernames and passwords to reduce the need for using insecure practices, such as writing passwords down, storing them electronically, or reusing the same login data on multiple websites repeatedly. These insecure practices can increase the probability of online crime, such as fraud and identity theft and, furthermore, can compromise the privacy of the individual. This chapter discusses a common network identity-verification method, called simplified sign-on, which allows users to roam between sites without having repeatedly to enter identifying information.

Chapter 4 looks at the effectiveness of Privacy Policy Statements (PPS). A PPS is a public notice of privacy and security practices in relation to the personal data held by companies. It is an important element in consumer trust, and in a consumer's decision to make purchases using Internet commerce services. PPS could, therefore, be expected to play an important role in overcoming the impediments to consumer purchases online. This chapter adds to the growing research literature on PPS by describing research involving comparison of an organization's PPS against a normative template developed based on professional practice and laws, policies, practices, and public expectations around the world.

Chapter 5 evaluates user password practice and determines that password-based systems are often compromised by poor user security practices. This chapter presents the results of a survey of 884 computer users that examines user practice in creating and reusing password keys, and reports the findings on user password composition and security practices for email accounts. Despite a greater awareness of security issues, the results show that many users still select and reuse weak passwords keys that are based on dictionary words and other meaningful information.

Chapter 6 looks at a case study of Wireless handheld device and LAN security issues in a healthcare setting. This chapter divides the ICT communications into wired and wireless technologies. The chapter concentrates on wireless technology and provides information on user acceptance of the technology in the healthcare industry. The major barrier to the uptake of wireless technology appears to be user concerns over various security issues including physical, logical, and data security.

Chapter 7 looks at Web 2.0 technologies for business solutions from a security perspective. This chapter discusses the business application of Web 2.0 and the security problems that can occur. Web 2.0 applications are the target for attacks from both external and internal agents and this chapter describes the background, applications, and security concerns of the Web 2.0 technologies used for digital businesses.

Chapter 8 looks at business continuity planning and explores the implications of the expectation that ICT systems need to be available 24/7 to internal and external users, regardless of the circumstances. This chapter discusses the nature of uncertainty in complex and dynamic environments and shows how this makes business continuity planning essential. The chapter argues that approaches such as virtualization can provide cost advantages to organizations by ensuring availability and resilience through flexible systems.

Chapter 9 looks at future trends in digital security. Technological predictions are notoriously uncertain but it is important to look forward and to outline some emerging directions. While it is too early to be definitive about specific technologies still developing, some current areas, such as wireless technology security, along with security policies and technologies around removable media, mobile phones and social networks, are covered briefly, and the applicable management principles are covered more generally within the book.

While this book offers valuable insights into the technologies that can help reduce the incidence of security breaches, in reality, the most important aspect of effective security is the human factor and employees doing the right thing with respect to the use of USB keys, accessing appropriate websites, and being vigilant about email attachments. This is the central message of this collection.

Don Kerr
University of the Sunshine Coast, Australia

John G. Gammack
Griffith University, Australia

Kay Bryant
Griffith University, Australia