DEFENDING THE DIGITAL FRONTIER

A SECURITY AGENDA

Mark W. Doll
Sajay Rai
Jose Granado

JOHN WILEY & SONS, INC.

DEFENDING THE DIGITAL FRONTIER

DEFENDING THE DIGITAL FRONTIER

A SECURITY AGENDA

Mark W. Doll
Sajay Rai
Jose Granado

JOHN WILEY & SONS, INC.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability of fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services, or technical support, please contact our Customer Care Department within the United States at 800-762-2974, outside the United States at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

For more information about Wiley products, visit our Web site at www.wiley.com.

ISBN 0-471-22144-9

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Contents

List of Figures and Tables

Foreword

Defending the Digital Frontier has been written to assist executives in the United States and beyond in understanding the critical nature of security within their organizations. While the focus of the book is digital security, which affects most if not all areas of business today, the book lays out an agenda for addressing a number of critical security risks, issues, and solutions.

Over the past year, President Bush has initiated a major effort to restructure the government and its agencies charged with supporting the homeland security of the United States. These plans, which streamline the chain of command and vastly increase the focus on security within both the federal government and the private sector, will greatly enhance America's ability to detect and mitigate threats and, when necessary, react to security incidents. The President's plans will bring a much needed comprehensive crisis management system to the federal government, including a structure for planning, preparing, and continuously practicing for security threats.

The time has come for senior executives of U.S. corporations to follow the President's lead and make security a mainstream, business critical, board-level issue—something it has not often been.

Like the federal government, senior executives must structure their organizations to address security threats. In most cases, organizations must create a new centralized framework that enables them to assess, design, plan, and implement security solutions for possible threats. Once organizations have taken these steps, they must continue to reevaluate their security posture through ongoing planning, preparation, and practice. This is a new era for American business. It calls for a new approach—a more secure approach. Corporate America's actions will in turn aid in the effort to secure America's homeland and in particular the critical infrastructure on which our economy, citizens, and governments rely.

This is not a situation that can be solved just by increasing corporate security budgets. In the past, security has been relegated to a line item on a balance sheet. Only if evidence of immediate return or the avoidance of serious financial exposure was evident would action be taken to secure the corporate infrastructure. From financial institutions to the energy, utility, healthcare, chemical, and transportation industries, American corporations are vulnerable. That means America is vulnerable.

Historically, many corporate security decisions, even for major organizations, are made not by senior executives, but by people with technical knowledge limited to their areas of expertise. Although they are no doubt dedicated to their responsibilities, they often have too little perspective to consider the impact of their decisions on the entire organization, and in turn upon America's critical infrastructure. The time when security-related decisions could be left to persons at the mid-manager level or decided solely upon budgetary consideration has passed. Senior executives must now take the steps to plan, prepare, and practice to address their organizational security threats and challenges.

Corporate security can only be improved if senior executives demonstrate commitment to the safety and security of their company, its assets, and its people. They must quickly assess the major security issues and the solutions available to address them. Business leaders across all industries must centralize their knowledge, standardize their response to incidents, and properly coordinate their efforts with one another and with all levels of government. It is integral that digital and physical security, crisis management, and business continuity be addressed as one strategic initiative.

The charge of securing corporate America falls upon its business leaders. This book, offered by Ernst & Young and written by Mark Doll, Sajay Rai, and Jose Granado, is not only timely, but comprehensive in outlook and broad in scope. It addresses many of the critical security issues facing corporate America today and should be read by responsible senior management.

THE HONORABLE RUDOLPH W. GIULIANI

Preface

The idea of a frontier brings to mind many images, all of which involve exploration, high risks, and high returns. The concept of a *digital frontier* adds another dimension of uncertainty because it is intangible. The means of getting to the digital frontier—the *hardware*—is the only tangible control associated with it. Everything else—the *data*, the *functions*, and, in the near future, the *means of distribution*—is, for the most part, without a fixed form. The digital frontier as we will define it has no territory and no outer limit other than that existing in the corporate imagination. Protecting the digital frontier is perhaps the greatest challenge facing business organizations in the early part of this millennium because digital security—the protection of *all* components of the digital frontier, including the human component—is complex, costly, and generally misunderstood.

The definition of digital security is amorphous because it affects so many aspects of daily life, yet it rarely produces the measurable return on investment realized by other information-related technologies; therefore, it is frequently ignored or devalued. However, in today's interconnected economy, digital security is a central, if not critical, element of business operations. Having in place a digital security program means an organization has chosen an integrated approach to protecting all of its digital assets: data, the media on which that data is stored, the devices used to create and store the data, and the medium or mode of transporting the data. It also means that the organization has chosen to protect the lives and livelihoods of the employees who use those digital assets in the course of day-to-day operations, to protect the mutual business interests of its customers and suppliers who rely on the availability and integrity of those digital assets, and to maintain the trust of its shareholders and the public who, for any number of reasons, must rely on the organization to preserve and protect the confidentiality of personal data. The consequences of failing to implement measures to protect digital assets can range from merely annoying to life-threatening. The magnitude of these consequences will only compound with the passage of time and the advent of new technologies.

Incidents over the past decade, whether successful or threatened, have highlighted the vulnerability of organizations to technological menace. For example, the Y2K fault, and the Code Red, Nimda, and I Love You worms failed to produce the information holocaust many security experts predicted. However, these threats caused damage estimated in the billions of dollars in downtime, loss of productivity, and repair and recovery efforts and affected almost every company in the United States and many more around the world. According to *Computer Economics*, the worldwide economic impact of the Nimda, Code Red, and Sircam attacks totaled $4.4 billion. The I Love You worm in 2000 inflicted an estimated $8.75 billion in damage worldwide, and, in 1999 the combined impact of the Melissa and Explorer attacks was $2.12 billion.[1] Affected organizations suffered real injuries in terms of money, image, and public confidence; however, the destruction was contained, mitigated, and even deflected in proportion to the effectiveness of the security measures companies had in place. The failure of such threats to cause even greater widespread destruction can be interpreted as a corollary to achieving a measurable return on investment in digital security.

To achieve the highest possible level of digital security, every member of an organization's executive management must realize that digital security is "baked in," not "painted on." Decision makers at that level must understand the need for digital security. Furthermore, they need a basic understanding of digital security and how it can be implemented within their organization. To that end, this book is intended to deconstruct digital security for executive management. It addresses the common problems of information protection for business organizations and it provides a framework in which to analyze and discuss digital security. It offers insight into the technologies, organizational issues, and processes that drive digital security and presents a set of mechanisms for identifying and managing risk to an organization's assets and people.

However, achieving and then defending security at the digital frontier requires more than just informed decision making at the top level. It also depends on the willingness of the executive management to change the organizational mind-set to a security orientation. A security-minded organization will be a secure organization. In this book, we describe what we consider to be the significant risks to an organization's digital security structure and explain why that structure's success relies as heavily on the organization and its people and processes as on technology. We offer a definition of world-class digital security and provide in-depth examples of what we consider to be its six key characteristics: It must be aligned, enterprise-wide, continuous, proactive, validated, and formal.[2] We describe how digital security can be achieved by designing it according to a detailed, proven, three-part Security Agenda: Restrict, Run, and Recover.^{SM}[3] We detail the nine items that comprise the agenda, which together enable any organization to achieve world-class digital security:

1. Intrusion and virus detection
2. Incident response
3. Privacy
4. Policies, standards, and guidelines
5. Physical security
6. Asset management
7. Entitlement management
8. Vulnerability management
9. Business continuity

We explain why digital security is no longer merely a technical function but a risk management operation requiring executive sponsorship, and is therefore dependent on a fluid strategy centered on identification and mitigation at the highest levels. Finally, we provide an approach for crafting, implementing, and supporting a pervasive security culture that is based on dynamic responsiveness in an evolving environment.

By strengthening the collective digital security knowledge base within an organization from the top down and enabling a clear understanding of the benefits of a comprehensive, inclusive, ongoing security agenda, every organization can build a secure future to the edge of the digital frontier.

MARK W. DOLL

San Jose, California
November 2002

Acknowledgments

We would like to thank two people without whom this book would not have been completed: Stephen L. Bates, contributing author, whose experience, keen insight, extensive knowledge of security, and many hours of research significantly contributed to the content and influenced the concepts in this book; and Mary A. Giery-Smith, technical writer, whose wordsmithing skills, editorial expertise, and ability to express technical concepts in a cogent, accessible fashion brought clarity to our message and enhanced the content of this book.

We would also like to thank the many others whose assistance was invaluable: Tikhon Ferris for his perspectives on IT risk management; Mark Moore, Scott Blanchette, and Gary Lorenz, who provided the shape of the book and much of the content presented in earlier drafts; Robert M. Roberge and Jeffrey L. Gill for their focus on a consistent security message; Christine Sharp for her efficiency and responsiveness as she assisted with graphics and tables; Sherry Flores, for all of her work behind the scenes to keep things organized and running smoothly; the other members of the 350 partners and staff of the Security & Technology Solutions practice of Ernst & Young LLP, whose support and encouragement added greatly to the success of this effort; and Debra Englander at John Wiley & Sons for her patience as this project came together.

M.W.D.

Part One
The Challenge of the Frontier

America has always been a land of frontiers that have been continually pushed, reshaped, and then pushed again. Since the evolution of America as a nation, we have been characterized by a restlessness and an unquenchable desire to discover, to tame and to lead. When the first European settlers arrived on America's eastern shore, they had no idea of the vastness of the land that lay before them. Even so, they migrated westward, secure in the knowledge that their collective future held enormous bounties as well as enormous risks. Later settlers, the pioneers who settled the American West, had a better but still incomplete understanding of both the risks and the rewards of redefining this young nation's frontiers.

The overwhelming majority of today's business organizations have invested enthusiastically in the promises of technological advances and have reaped the benefits of productivity gains. As they entered the twenty-first century, these organizations were firmly entrenched in the digital age by virtue of having achieved a high degree of reliance on information technology (IT). Some organizations rushed to the edge of the digital age, to its very frontier, and have become leaders by adopting and utilizing the latest technologies and achieving a high degree of reliance on them. Other firms closely followed these early adopters; others trailed much farther behind.

Despite the widespread use and reliance on new technology, however, this vast new frontier is just as unevenly explored as the American West of the 1800s. Some areas of information technology, such as mainframe security, are well established; the risks are understood and have been addressed. Newer technologies, although heavily relied upon by organizations and their employees, customers, and suppliers as part of the daily routine, nevertheless contain inherent risks that are less well understood by the average user. Examples of these technologies are e-mail systems, the Internet and World Wide Web, and private networks. These technologies have become essential elements of everyday life in corporate America and, indeed, in the global economy.

Just as the familiar laws and infrastructures in the young cities of the American West provided some comfort to nineteenth-century settlers, twenty-first century businesses have found comfort in knowing that somewhere within their organization an IT department has implemented little-understood security countermeasures to protect the organization's information assets from hackers and other malcontents. However, this sort of thinking is naïve. The digital frontier is dynamic; it continues to expand. In many cases, if not most, it has already expanded beyond the ability of organizations to protect themselves from real threats. The security capabilities of companies at the digital frontier should have expanded at the same rate or faster to provide comprehensive protection, but they have not.

When the western pioneers left the cities for the wilderness, more than just the landscape changed. The risks changed. So, too, for today's business organizations. The digital frontier is as unsettled as the frontier faced by America's expansionist settlers with two stark differences: The digital frontier is not a territory on a map, and there is no law of the land.

The digital frontier is virtual and borderless. There are no common rules of engagement that will protect its pioneers, and the standards for recourse or redress are just as inconsistent. However, underlying these differences is one striking similarity between the frontiers that has remained unchanged for more than a century. It is the problem of how to prepare to face things that cannot be predicted or even imagined. Firms that want to reap the benefits of being at the digital frontier—increased productivity, market dominance, and increased customer satisfaction—must be prepared to defend their assets and their people against a variety of security threats that may strike without warning, and may leave little room for recourse other than retrenchment.

Part One describes the challenges facing the most senior stakeholders in the global economy—executive management—whose decisions about digital security today will produce effects that will be felt for years to come. The first two chapters provide an in-depth discussion of how an organization can determine its position with regard to the digital security frontier and an overview of the key characteristics of digital security. The third chapter addresses the issue of resource allocation, including personnel, and provides a context for executing the critical technologies, organizational enhancements, and necessary processes that will enable a firm to achieve digital security. Together, these chapters present the foundation of a cyclical strategy to successfully defend an organization's stake in the digital frontier.

1

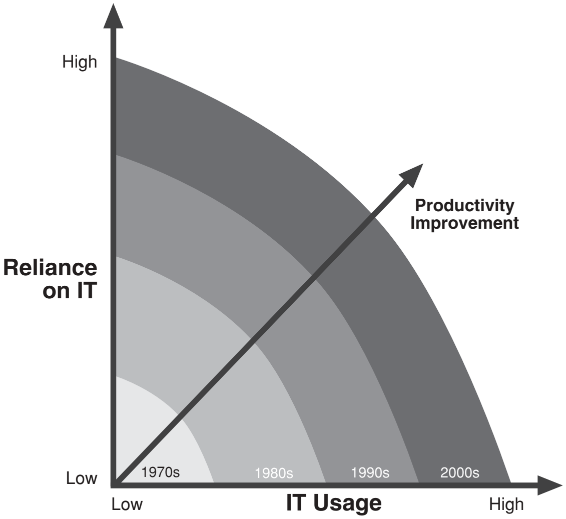
The Security Frontier

In the introduction to Part One, the digital frontier was described as virtual, borderless, and highly dynamic. By implication, its environment is fluid rather than concrete, and transitory rather than fixed. Although such terms lend understanding in the abstract, they are less helpful when trying to quantify the frontier. Therefore, we offer the following operational definition of the digital frontier: *It is the forward edge of technological impact with respect to organizations' usage of technology and their reliance upon it for day-to-day operations to achieve marketable productivity improvements* (see Figure 1.1).

It is important to understand the difference between the "bleeding edge" of technology and the digital frontier because, although they have similarities in terms of their positions at the forefront of innovations with respect to the majority of business organizations, there are several significant distinctions. Companies investing in so-called bleeding edge technologies have as one of their drivers the adoption of the latest technology for experimental purposes. Companies investing to the edge of the digital frontier are careful to adopt the latest and best technology available *with regard to its utility and performance because usage and adoption are critical to productivity gain.*

Just as settlers pushing the boundaries of the American West redrew the maps to show later explorers where the old frontiers had ended and

FIGURE 1.1 The Digital Frontier



which areas were still open for development, Figure 1.2 shows the four clearly distinguishable eras on the continuum of digital technology. These eras are defined by their architecture, and all were pushed forward by the companies whose executive management understood that there must be a direct correlation between digital investment and operational productivity. Those executive managers knew that a high degree of both usage and reliance is what puts an organization squarely in the digital frontier, and their companies are the ones that traditionally have and are still holding the competitive advantage in the marketplace. The eras shown in Figure 1.2 can be described as follows:

1. *Mainframe:* This era is characterized by highly centralized systems and closed architecture. This era was the advent of the digital age, beginning with the development and use of the Electronic Numerical Integrator and Computer (ENIAC) in 1947.