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

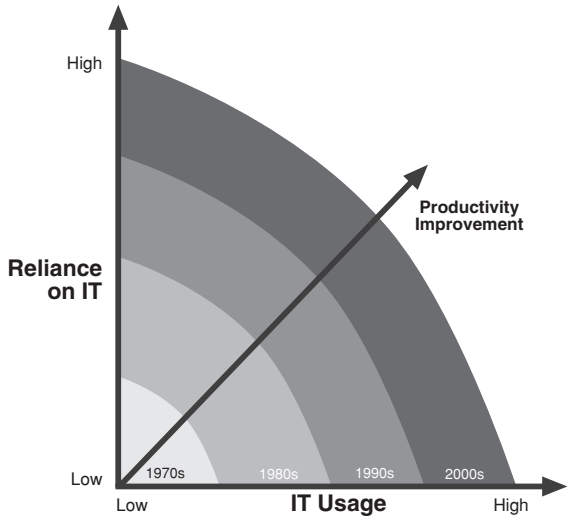
The Security Frontier

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

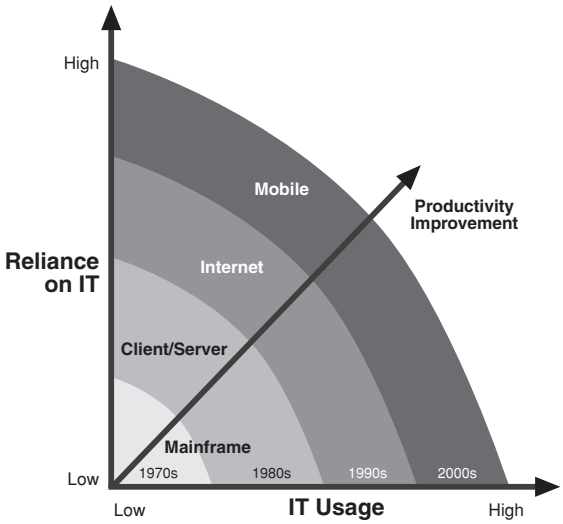
FIGURE 1.1 The Digital Frontier



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.

FIGURE 1.2 Computing Eras That Have Shaped the Digital Frontier



Mainframe systems evolved, but continued to be the platforms of choice until the mid-1980s.

2. *Client/server:* This second major shift along the digital frontier ushered in the concept of distributed information, private users, and decentralized systems. This has proved to be an enduring structure and is still in widespread use today, with adaptations for more advanced technology.
3. *Internet:* The concept of a highly decentralized, open-architecture system that connected widely distributed users had been in use for a decade or more in the form of the original Advanced Research Projects Agency Network (ARPANet) of the U.S. Department of Defense, which connected academic and military research institutions. However, in the 1990s, this network was opened for public access and its usage increased exponentially. By the end of that decade, reliance upon it had become ubiquitous for business

and non-business-related usage. Companies that had previously lagged behind in terms of technological innovation went online in the 1990s.

4. *Mobile:* The fourth wave of innovation, the effects of which are beginning to be felt in the business world at the beginning of the twenty-first century, is the era of wireless communication via highly decentralized, open-architecture systems. This technology is reshaping the digital frontier as wireless technology segues from being at the bleeding edge of technological innovation to the leading edge of the digital frontier. Organizations have begun to study its utility and determine their potential to become reliant upon it. The key factor in how ubiquitous this technology becomes will be its ability to significantly increase productivity without increasing risks to the organization's security framework.

The greatest danger facing organizations that exist at the digital frontier is one of their own making. The last decade of the twentieth century saw an explosion of development in high technology. Microprocessors allowed information to be created, stored, sorted, and reassembled at speeds measured in nanoseconds, and fiber-optic technology enabled that information to be transferred literally at the speed of light. The time lapse between generations of the microchip decreased from being measured in years to being measured in months. Portability became an issue, and the convenience of independent, interconnected desktop workstations was surpassed by laptops, which were in turn surpassed by smaller, sleeker notebook computers. By the end of the century, powerful computers with nearly full functionality fit in a shirt pocket.

Nearly every industry underwent a dramatic evolution as new technologies helped to streamline productivity and increase efficiency. These technological advances fostered a dramatic surge in spending as businesses of every size and description invested heavily in upgrading their IT systems. The ability to digitize information had truly revolutionized the way companies conducted business. Increased usage and

increased reliance were viewed as part of a reward cycle that would yield higher productivity and lower associated costs. However, with the precision lent by hindsight, we can now view this behavior by companies at the edge of the digital frontier from the perspective of risk rather than reward. Consideration of the situation from this viewpoint reveals that the closer a company is to the edge of the digital frontier, the greater the probability of failure of the systems relied upon, and the greater the impact of that failure when it occurs. This is *security risk* (see Figure 1.3).

When an organization's security risk (probability and potential impact of failure) is superimposed on productivity (an organization's usage of and reliance on technology), a new frontier emerges. We call this the *security frontier* (see Figure 1.4). Its parameters are measurable, and they are different for every company; therefore, defining it is not difficult. Defending it, however, is nearly impossible.

FIGURE 1.3 Security Risk

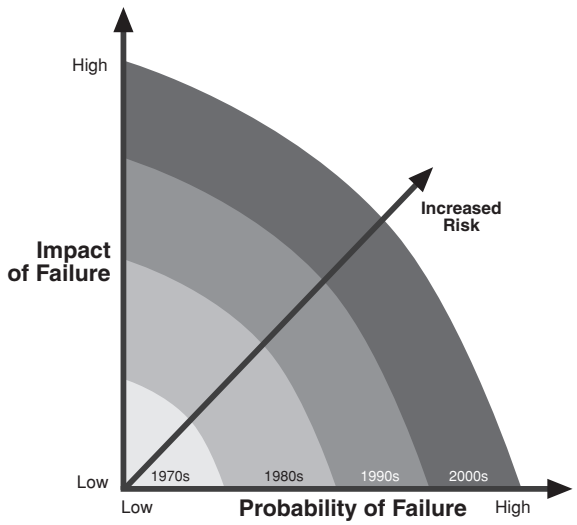
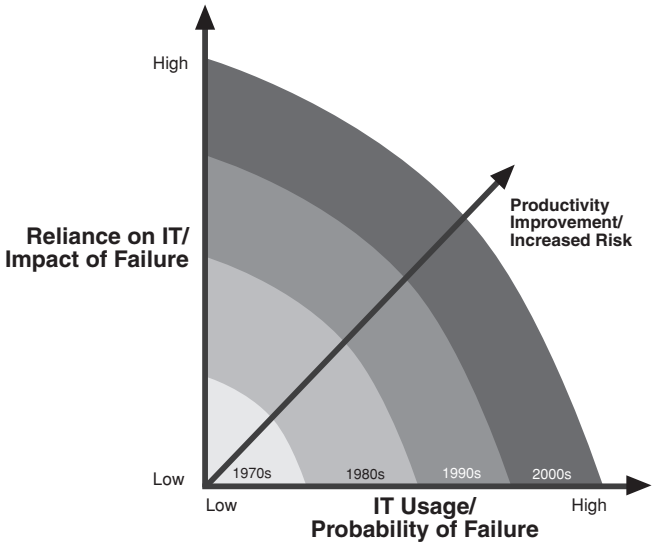


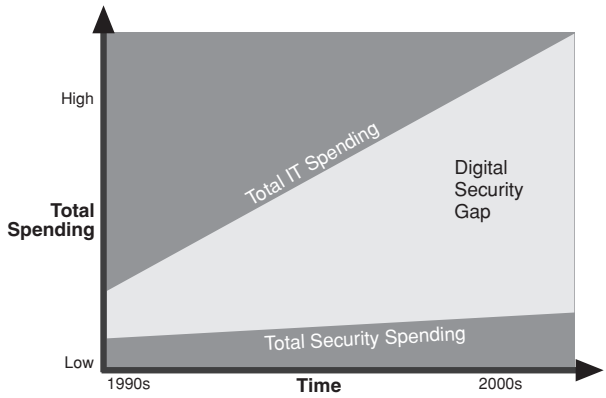
FIGURE 1.4 The Security Frontier



Caught up in the enthusiasm for becoming "wired" in the late 1990s, few companies stopped to consider the consequent vulnerabilities of opening their formerly closed information systems. Even fewer spent proportionally on defending themselves against attacks. This exuberant spending and unintended shortsightedness coalesced to form what we call the *digital security gap* (see Figure 1.5).

The challenges associated with the digital frontier must be identified, acknowledged, and managed in order for organizations to defend against them while maintaining their position at the frontier's leading edge. Defending the digital frontier requires that organizations encourage an evolution within their digital security programs. Detailed descriptions of this evolution are discussed in Chapter 3 and Chapter 8. However, the foundations of this evolution are among the largest challenges facing organizations at the security frontier and are discussed in the following sections.

FIGURE 1.5 The Digital Security Gap



IDENTIFYING THE SECURITY FRONTIER

Meeting the dual challenge of remaining at the edge of the digital frontier while closing an organization's digital security gap requires an understanding of what being at the digital frontier means to the organization, as well as an awareness of how the organization can defend its position there. It means executives should know everything they can about their organization's security frontier and what risks their organization faces. However, nobody can provide that information. To be completely secure, to be completely safe, the executive management of an organization must know what they can't possibly know.

An ***information asset*** is information possessed by an organization during the process of conducting business. The information may be owned by the organization, for example, customer lists, or it may be information placed under the custodianship of the organization for a specified period of time, for example, a credit card number provided by a customer to complete a business transaction.

A ***digital asset*** is information stored or processed on or by digital media and the corresponding physical and logical devices used for storage, processing, or transport. Examples of digital assets include computer hardware and software, computer hard drives and the data stored on them, and a network and the range of a wireless hub. Digital assets must hold some level of value to stakeholders or be governed by a law or regulation in order to be classified as assets.

Eliminating all threats to and vulnerabilities affecting an organization's digital assets is impossible as well as impractical, just as it is impossible and impractical to secure a nation's borders by building a perimeter so secure that it impedes the flow of commerce. However, securing those assets is both possible and practical. Achieving digital security, much like achieving national security, becomes an exercise in identifying, mitigating, and tracking threats and vulnerabilities and repairing breaches. The work is cyclical and continual, and in order to engage in it effectively, executive management must know what information assets are at risk and understand the organization's current digital security requirements, as well as its current digital security capabilities.

Environment

The digital frontier can be entered unknowingly. Upgrading a system or adding new technologies or components can initiate movement along the digital technology continuum, introducing significant risk to an organization's digital security. A broad understanding of the firm's digital information assets and operations is required in order to determine where an organization exists at the frontier; this knowledge will enable the organization to identify and mitigate that risk. The first step in facing the challenge of the digital frontier is to *determine where an organization is with regard to the security frontier.*

Identification of an organization's position relative to the security frontier involves more than just knowing the basic foundation of its computing resources in terms of usage and reliance. There must be a

detailed understanding of why the organization occupies that position on the frontier. Specifically, senior management must understand which assets are being protected and why. What are the issues or requirements driving the organization's utilization and reliance on digital technology? What are the current capabilities of the digital security program in place?

The criticality and sensitivity of information assets may be, but are not necessarily, correlated.

Sensitive information assets are those that could, if compromised, pose grave threats to the organization. Examples of sensitive information include unannounced strategic decisions, human resources information, or intellectual property, such as research and development data.

Critical information assets are those upon which the organization relies to conduct routine business, for instance, to generate revenue and facilitate communications or transactions and could include sensitive and nonsensitive information. An example of critical but not sensitive information would be sales tax information for a retailer—information that is critical to running the business, but the release of which will not compromise the organization.

What information is worthy of protection? Does all of an organization's information require the same level of protection? Where is the most important information stored? For instance, is an organization's most critical or sensitive information stored in databases created using shrinkwrapped applications? Which version of the software is being used, and are all the copies licensed? Is the software installed on one server, or twenty? In which office or offices are the servers located? Who owns the database, and who determines who gets access to the data in it? How frequently is it backed up and where are those backups stored? These are questions that the IT personnel in an organization should be able to answer quickly. But do those IT specialists understand the value of the information? Should they? Should IT be the only repository of that information?

The identification of information assets is one element of understanding where an organization exists with regard to the security frontier. This identification must involve the IT department, certainly, but it is also a function that must be understood and undertaken by management at the highest levels. After all, implementing every high-technology security precaution available cannot prevent unauthorized access to a sensitive database stored on a remote server if no one is aware that the server exists. This is why comprehensive asset identification must be addressed with the same gravity as is given to an organization's security capabilities and its security requirements when planning to deploy a digital security program.

The second part of the asset identification issue is understanding who or what sets up the security issues. In other words, how are an organization's digital security requirements determined? Is an organization bound to comply with federal security regulations, including privacy regulations?[1] Do business partners impose specific technical security configurations on an organization's external networks? What would be the impact of an unintended release of sensitive or critical information?

> ***Privacy*** is the right of an individual to determine to what degree he or she is willing to disclose personal or other information about him- or herself. When such information is provided to other entities, individuals, or organizations, this right extends to the collection, distribution, and storage of that information.

Every organization has its own mix of regulatory-, industry-, and internally driven digital security mandates; therefore, the answers to these questions are key to determining an organization's digital security requirements. Typically, external mandates can be obtained from clearly defined sources. Within the healthcare industry, for example, the security and privacy of patient information are addressed by the Healthcare Insurance Portability and Accountability Act (HIPAA) of 1996 and other federal and state regulatory requirements. Similarly, in the banking and financial industries, the Gramm Leach Bliley (GLB) Act of 1999 and

other regulations set requirements to protect customer information.[2] Internally driven requirements are typically less clearly defined, and frequently organizations must initiate far-ranging audits or assessments to determine them. Once understood, these mandates can serve as a foundation for determining digital security objectives and as a framework for measuring how well those objectives are being met.

Examples of Federal Laws Impacting Security Considerations

- Patriot Act of 2001
- Digital Privacy Act of 2000
- Electronic Communications Privacy Act of 1986, 2000
- Gramm Leach Bliley (GLB) Act of 1999
- Electronic Freedom of Information Act of 1996
- Healthcare Insurance Portability and Accountability Act (HIPAA) of 1996
- National Information Infrastructure Protection Act of 1996
- Computer Security Act of 1987
- Computer Fraud and Abuse Act of 1986
- Computer Crime Control Act of 1984
- Privacy Act of 1974

Once the critical and/or sensitive information has been identified and the security mandates for protecting those assets are understood, the state of an organization's existing security capabilities must be considered. What does that firm's digital security program look like today? For instance, how is the network monitored with regard to unauthorized access? What is the process for providing new personnel with user access to Internet applications? What is the security configuration for the payroll application? Who has been given responsibility, direction, and authority to perform digital security functions? Most importantly, could the models on which the answers are based be considered best-in-class?

Responsibilities

For each of the past seven years, the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) have surveyed large U.S.

corporations, government agencies, and financial, medical, and academic organizations about digital security issues. The results are published as the annual *CSI/FBI Computer Crime and Security Survey.* One of the more chilling statistics presented in the survey is that of the 98 percent of respondents that have World Wide Web sites, 21 percent *did not know* whether there had been unauthorized access to or misuse of their site in the preceding 12 months.[3] Although it is inappropriate, this lack of understanding is not surprising. However, it is inexcusable for an organization operating at the digital frontier; in the near future it may be actionable. That is why the second step in identifying an organization's security frontier is to *define executive management's responsibilities* with regard to defending the organization's position at the digital frontier.

> ***IT governance*** refers to the oversight and guidance of information and applied technology within the business and business-related fields by stakeholders, which can include an organization's directors and senior management, as well as process owners and IT suppliers, and users, and auditors.
>
> *—Board Briefing on IT Governance, IT Governance Institute*

Management responsibilities for digital security are but one component of corporate responsibilities for IT governance. According to the IT Governance Institute, which provides guidance on current and future issues pertaining to IT governance,[4] the responsibility for IT governance lies with the board of directors and executive management. Such governance "is an integral part of the enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives."[5] Specifically, management must address "[t]he risks of doing business in an interconnected digital world and the dependence on entities beyond the direct control of the enterprise; IT's impact on business continuity due to increasing reliance on information and IT in all aspects of the enterprise"; and, "[t]he failures of IT," which are having an increasing impact on reputation and enterprise value.[6]

In today's global, digitally-linked marketplace, executive management has a fiduciary responsibility to shareholders as well as a responsibility to the organization. The latter responsibility is operational in nature—to ensure the continuation of business in the face of threats and attacks. It is the responsibility of executive management to deploy a digital security program that enables management to determine which risks to accept, which risks to mitigate, and which resources to deploy toward that mitigation. Carrying out these responsibilities entails the following:

- Setting the objectives for digital security.
- Allocating resources for a program to achieve and maintain digital security, including monitoring and measuring the program itself.
- Promoting a digital security culture.
- Reducing the total risk of security failures while eliminating high-impact events.
- Conceiving a charter for the digital security program that establishes goals and standards for an implementation framework.

Priorities

The nature of threats and vulnerabilities at the digital frontier will be discussed later in this chapter. However, any attack at the frontier can be guaranteed to have two characteristics: speed and severity. When a firm's information system is successfully attacked, whether the attack is made to its networks, its website, or any other subsystem, more than just information is compromised. Trust has been lost at every level. An organization's structure, its internal culture, and its corporate image are affected, and the repercussions may be most strongly felt with regard to consumer confidence and in turn, on the bottom line. Therefore, the third step in facing the challenge of the digital frontier is to *define executive management's priorities* in defending an organization's position at the frontier.

Earlier in this chapter, information was introduced regarding an organization's digital security requirements and capabilities, and how

best to identify its digital information assets. This section raises the same issues but from a management perspective. For instance, what is the real threat to an organization under or facing an attack? What will be the direct, immediate business impacts of a release of sensitive or critical information? Will all means of entry to the system have to be shut down? If so, for how long? What is the intended target of the attack? What can be compromised in an attack: shareholder and consumer confidence, brand image, share price, or safety of personnel? Which assets are controlled by systems, and what would be the effect of the failure of those systems? Is the organization security-minded? Who in the organization understands the technology? What are the options with regard to defense? How fast is fast enough when you're talking about responding to a breach of security? How much is enough to spend defending an organization's position at the digital frontier? What is the return on investment of implementing security measures?

Executive management's priorities are found in the answers to these questions. The challenge lies in determining what to do *before* a crisis strikes, and then doing it continuously. This necessitates an entire organization adopting a security mind-set. It also requires that executive managers learn more than just the technical terminology of an organization's digital security program; they must have at least a basic understanding of what digital security means, what it involves, and what such a program can and cannot achieve. The less executive managers understand about both the technology and the solutions, the more *unwarranted* decision-making power they may be placing in the hands of technical people whose scope may be limited with regard to an organization's goals and needs. This delegation of authority to persons who may not understand the business risk versus the business return is inappropriate, and possibly dangerous.

There are no "right" answers to the questions asked in this chapter. The responses will vary for every organization depending on the industry, the product or products produced by the organization, the organization's reliance on technology, and the type of technology in use by the organization. Therefore, the priorities for every organization will be

different, as will the options available to them in the planning stages. The goal, however, should be the same: to build a digital security program.

CHALLENGES AT THE FRONTIER

Information has always possessed an inherent value. As a result, information security is not a new phenomenon. Evidence suggests that information protection is nearly as old as civilized society. Ancient Egyptians, Greeks, and Romans demonstrated varying degrees of encryption and decryption expertise in an effort to keep sensitive information secret. Although the practice of protecting information from unauthorized access, modification, or compromise has changed little over time, the methodology has changed dramatically.

Many traditional barriers to information exchange do not exist in today's business environment. Access to sensitive data no longer requires physical proximity; data exists in smaller spaces and can be stored on increasingly compact, easily transportable media and can be transferred by wireless means. The benefits of speed and portability are balanced by the knowledge that information is more accessible and less protected than ever before. The rush to continually extend the boundaries of the digital frontier, to meet increasingly aggressive operational objectives in shorter periods of time, has left many business organizations in the precarious position of having more information assets open to compromise than ever before as they try to retrofit their existing digital security apparatus and countermeasures to meet today's security needs.

Threats and Vulnerabilities

Once an organization has identified its place at the digital frontier and executive management has defined its responsibilities and priorities with regard to defending that place, there is still a group of unknowns to consider. The unknowns in this case are a loose collection of issues called *threats* and *vulnerabilities.* Threats to and vulnerabilities of an

organization's digital security program are two sides of the same coin. Both are capable of inflicting extreme damage, and both may be effectively deflected with prescriptive vigilance and reactive diligence.[7]

Four Broad Categories of Threats

- *Interception:* Data is siphoned from the system.
- *Interruption:* Networks and Internet access are rendered unusable in a denial-of-service attack.
- *Modification:* Authorizations or access codes are changed.
- *Fabrication:* False information is inserted into a system.

A threat to an information system is any act upon or against the system that is performed with the intention to cause harm. Threats can be internal or external to the organization; they can include human threats, such as disgruntled employees, or they may be derived from vulnerabilities, such as a remote server no one is aware of. *Vulnerabilities are generally inherent weaknesses in an information system,* although some vulnerabilities may result from deliberate acts or omissions. Despite peer review, little commercial software reaches the market free from vulnerabilities, and even systems developed in-house frequently achieve full-scale implementation prior to the detection of potential vulnerabilities. Potential avenues of attack are discovered almost daily, and such information is freely disseminated among the IT community and other interested parties, including potential intruders or hackers.

Common Causes of Information System Vulnerabilities

- A developer's risk-versus-reward analysis.
- Development efforts that focus on performance rather than security.
- A systems designer's inability to predict potential targets for exploitation.
- Inefficient change control.
- The average user's misperceptions about security risks.
- Misunderstandings about security protocols and the need for them.

According to the 2002 CSI/FBI Survey, "the threat from computer crime and other information security breaches continues unabated and the financial toll is mounting."[8] Ninety percent of the survey's respondents had detected computer security breaches within the 12 months preceding the survey, and 80 percent acknowledged financial losses due to those breaches.[9] The 44 percent of respondents that were willing or able to quantify their losses reported an aggregate $455 million worth of damage.[10] The most serious areas of loss were the theft of proprietary information, which totaled $170 million, and financial fraud, which totaled $115 million. The highest individual loss due to theft of proprietary information was $50 million; the average loss was $6.57 million.[11] The highest individual loss due to financial fraud was also $50 million; the average loss was $4.6 million.[12] Insider abuse of Internet access, for example, employees' use of company computers or access to download pornography or pirated software, or the inappropriate use of the organization's e-mail system, cost respondents $50 million.[13] Despite a high proportion of antivirus software implementation, viruses and their aftermath were detected by 85 percent of respondents and carried a price tag of $49.9 million.[14]

As this information shows, the risks are real and the stakes are high. It is incumbent upon the executive management team to understand what they are facing as they stand at the edge of the digital frontier. An organization operating at the security frontier must understand that its place is a dangerous one. It has a landscape that changes, and with each incremental change, everything changes. This means that although any group or system within the organization can be the component leading the organization into the frontier, that component may be the vulnerable area, or it may cause a vulnerability to be overlooked. All it takes is one person who doesn't "get it" to cause a security breach that can take vast amounts of time, money, and manpower to fix and that can have grave repercussions in the marketplace.

There are obstacles beyond threats and vulnerabilities that present challenges for organizations at the edge of the digital frontier. Many of these obstacles are the product of misperceptions that can influence organizations in many ways, permeate the decision cycle from the

executive to the user level, and undermine security efforts. Examples of these misperceptions include:

- Information security efforts are an IT domain, or the purview of a specialized security group.
- Security threats and vulnerabilities are unique to high-profile industries or companies.
- Outsiders compromise information most frequently, and such compromise is often detected and prosecuted.[15]
- Security policies are sufficient to guide operations in a secure manner.
- Security technology will solve security needs.
- Security impairs organizational objectives and serves as a barrier to progress.

An Attack Scenario

Many threats exist on the digital frontier. Unfortunately, many companies have digital security programs that may be, in themselves, a serious vulnerability with regard to their ability to identify threats and address vulnerabilities in a way that mitigates the impact of digital security incidents, and their ability to respond appropriately when an attack occurs. Consider the following real-world scenario and some of the questions it raises from the perspective of an executive who thought the organization was secure.

Stage One: Onset and Initial Response

An employee who has been with a major healthcare services firm for 15 years leaves the company under less than pleasant circumstances. Shortly thereafter, her former coworkers and others complain that their passwords on certain corporate systems, such as e-mail, are no longer working. It is known that the ex-employee had knowledge of those systems, including default or known passwords, and there are indications that she has used that knowledge to access components of those systems. In an effort to resolve the situation, IT management issues an urgent request

for employees to change their system passwords. Some employees respond appropriately and change their passwords; others ignore the request. At this stage in the scenario, several issues have been raised:

- The organization's policy regarding removing employees from the system when they leave is not being followed, nor is the organization's policy regarding requiring employees to change passwords on a routine schedule.
- The organization's policy regarding the use of corporate applications that rely on default or hard-coded passwords at the system level—in other words, critical application functionality will break if the passwords are changed—has been shown to be a vulnerability, and there is apparently no policy restricting systems from using hard-coded passwords or requiring implementation teams to change default passwords prior to going live with systems.
- The decision to shut down compromised systems or disconnect them from the Internet must be considered. Does current policy indicate the party responsible for making that decision, and does it address the impact of that decision on business?

Stage Two: Information-Gathering and Option Analysis

Because the ex-employee has gained illicit access to the e-mail system, the potential exists that other Internet applications also may have been compromised, such as the firm's online subscriber information database. Some of these applications may have default passwords that are crucial to their operations. The ex-employee may know these default passwords, or she also may know other employees' passwords to these applications. As a response to this potential issue, programmers and vendors for the potentially compromised applications are contacted. They report that changing certain passwords on some systems is possible; however, it will take a month or more to make necessary programming changes and conduct remedial testing. The one-month time frame will affect the availability of the applications—perhaps even requiring that they be taken offline, which would necessitate a public

explanation. This time frame will require adjusting the priorities of the current IT staff, thereby affecting the timeline of other projects currently underway.

Meanwhile, system and security administrators have put extra resources into the effort to determine how she is accessing Internet systems, but have little to show for their efforts. Some of the organization's information systems are configured to log activity; others are not. However, even those systems that log information are only logging certain events, for example, failed logins. They offer nothing in this situation because the ex-employee is not failing to log in; she knows passwords and she knows the system's "back doors." She knows where the system's holes are, which means she could change security configurations on the systems and no one would know. This raises the following additional issues:

- There are no implemented policies for logging security events on all systems or for accountability with regard to monitoring those systems.
- Without knowing which systems have been compromised, the organization cannot learn whether data has been modified, stolen, or deleted, or whether sensitive or critical information, such as customer data or information regarding business partners, has been compromised.

Stage Three: Escalation

Five days have elapsed since the first security breach was discovered. The ex-employee is still accessing corporate systems and changing employee passwords. She has hijacked the e-mail account of a current employee and uses it to send an internal e-mail to management. This e-mail, appearing to come from a current employee, complains that the ex-employee was "let go" unfairly and "did nothing wrong." The issues under discussion have become broader in tone, and more urgent:

- Activating the business continuity or disaster recovery plans is considered.

- The decision to contact law enforcement is considered, as well as the public relations ramifications of taking that step.

Stage Four: Malicious Escalation

The ex-employee sends another e-mail to selected company managers; this one contains an agenda. It reveals that for some time she was frustrated by the firm's lack of security and that "no one listened" to her attempts to address it. Now, she has their attention. The e-mail further reveals that she is in possession of patient healthcare histories and intends to disclose the information to the public, just to show how insecure the company's environment is.

At this juncture, the scenario could move in several directions. However, the point has been made that the well-being of the organization has been placed in grave jeopardy by the actions of one person who may have limited but critical knowledge of the system and perhaps only ordinary computer skills. This scenario or one eerily close to it could be played out in any large company in any industry at any given time. Executive-level managers and corporate officers must ask themselves how it would be handled if it happened at their firm:

- Would the digital security program currently in place have the resources to find the necessary answers, and do so in a timely and organized fashion?
- Would prior decisions made by executive management about digital security empower or hinder those responsible for digital security as they sought to find solutions?
- What would it cost to address this scenario?
- What would shutting down a busy web site for 24 hours cost in terms of lost revenue, not to mention the damage to the organization's public image?
- What are the legal ramifications of having sensitive private information publicly released?
- What would it cost to have system administrators spend hundreds of hours investigating the incident and rebuilding compromised systems?

- What would it cost to have administrators and senior management spend dozens or hundreds hours in meetings during and after the incident?
- What would it cost to have the public, government, and media relations departments spend hundreds of hours working on damage control plans and collateral materials intended to restore decreased customer and shareholder confidence?
- How much will the stock price drop, and how long will it take to rebound?
- Worst of all, what if such an attack happens again before the organization has a new program in place?