PART ONE

The Challenge of the Frontier

The desire to expand the bounds of knowledge has always led mankind to unknown frontiers. In the second half of the twentieth century, with the Earth well mapped, we left the protection of the atmosphere and opened a new frontier in outer space. The dawn of the space age coincided with the dawn of the information age. As space pioneers advanced from Sputnik to the space shuttle, global businesses started to explore the digital frontier by investing heavily in information technology and striving to reap the benefits of competitive advantage.

In many ways, the digital frontier is as unevenly explored as space. Some areas of information technology, such as mainframe security, are more likely to be well-established and the associated risks are better understood. Newer technologies, although heavily relied upon by organisations as part of a daily routine, contain inherent risks that are not as well understood.

A challenge that faces pioneers of both the space frontier and the digital frontier is preparing for risks that cannot be predicted or even imagined. Companies 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 threats that may strike without warning. This may leave little recourse other than retrenchment.

Part One of this book describes the challenges facing executive management, whose decisions about how their organisations defend themselves at the digital frontier today, will produce effects that may be felt for years to come. Chapters 1 and 2 provide a discussion of how an organisation can determine where its digital frontier exists and an overview of the key characteristics of digital security. Chapter 3 addresses the issue of resource allocation including personnel, and provides a context for deploying the critical technologies, organisational enhancements, and necessary processes that will help an organisation in its pursuit of digital security. Together, these chapters present the foundation of a cyclical strategy to successfully defend an organisation's position at the digital frontier.

1

Living at the Digital Frontier

- Increasing Complexity
- The Digital Security Gap
- Mapping the Digital Frontier
- Challenges at the Frontier

The desire for increased profit and competitive advantage has always pushed business to adopt technological advances. Mechanisation, clipper ships, railroads, electricity, the telegraph, the telephone, computers, and the Internet have all brought step changes in productivity and efficiency that have led to improved bottom-line results. As the speed of technological advance, especially in information technology (IT), has increased in recent years, organisations have continued to take up the latest tools—whether or not they fully understood the associated risks.

This widespread use of IT has led to a sort of "digital frontier," a dynamic place where each organisation reaps the benefits of instant information access and increased productivity yet at the same time faces new and complex dangers. Some organisations choose to position their digital frontier at the "bleeding edge" of technology; they use the very newest, often still experimental technologies in speculative attempts to

secure advantage over their competitors. Others take more conservative approaches, adopting new technology when the benefits and risks are more clearly understood. But no matter where an organisation chooses to establish its digital frontier, it must understand that there are risks and changes that need to be identified and managed at a senior level.

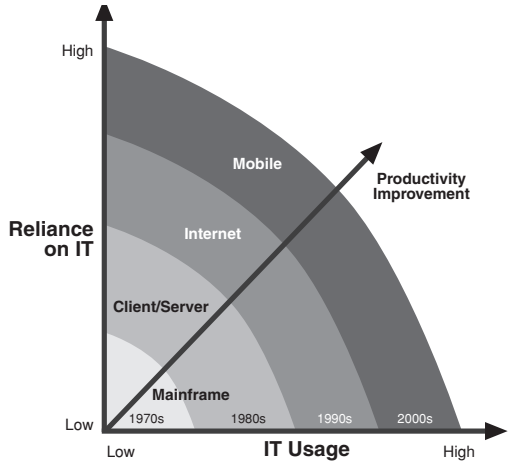
INCREASING COMPLEXITY

To understand how these risks have multiplied during the information age, it helps to trace briefly the history of the business world's use of IT and its increasing complexity. When organisations first started using computers, those computers were huge machines that took up their own vast rooms. The hardware, software, and operations were all housed in clearly identifiable facilities, and it was relatively easy to define what needed managing and who could access it.

With advances in processor power and miniaturisation, computers in the 1970s and 1980s moved out of the well-defined physical boundaries onto servers and desktops distributed throughout the organisation. The security risk was multiplied, but the networks were relatively simple; understanding what was connected to each network and how to manage it was relatively straightforward. The increasing complexity and reach of corporate networks however, brought a raft of new security challenges based around connectivity. These challenges increased as corporate networks came together in the biggest of all networks, the Internet, and linked to the networks of customers and suppliers. Compounding this, desktop machines were supplemented by laptops, notebooks, and personal digital assistants (PDAs), all of which moved out of the office and enabled employees to work anywhere, anytime (see Figure 1.1). The network is constantly changing, parties beyond the organisation's perimeters have access, and users control their own devices.

It has become increasingly challenging to understand what comprises security and who is responsible for it. With each step forward, flexibility and utility have increased, but so has complexity. In the 1970s, defending an organisation's IT infrastructure was not much more com-

FIGURE 1.1 Businesses' Usage of and Reliance on Information Technology (IT)



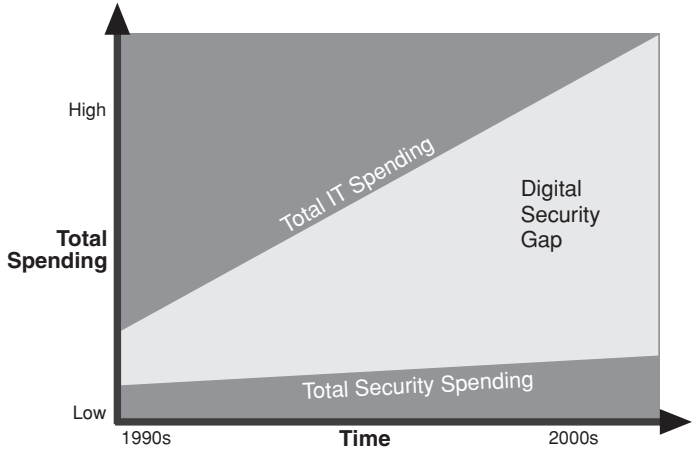
plicated than making sure the computer room had a good lock on the door. Today, a corporate network includes not only the machines physically wired together around different offices, but also thousands of devices connected over remote telephone lines, wireless fidelity (wi-fi) hotspots, and via Bluetooth connections or to mobile phone networks.

THE DIGITAL SECURITY GAP

As complexity increased and risks multiplied, few organisations properly considered the new risks they were taking on. Even fewer spent proportionally on mitigating these risks. This has created what we call the *digital security gap* (see Figure 1.2).

The challenges associated with the digital frontier must be identified, acknowledged, and managed for organisations to defend against them while maintaining their position at the frontier. Defending the digital frontier requires that organisations encourage an evolution within their security programmes. Detailed descriptions of this evolution are pre-

FIGURE 1.2 The Digital Security Gap



sented in Chapter 3 and Chapter 8. However, laying the foundation of this evolution is vitally important and is discussed in the following sections.

MAPPING THE DIGITAL FRONTIER

Meeting the dual challenges of remaining at the digital frontier while closing an organisation's digital security gap requires an understanding of what being at the digital frontier means to the organisation, as well as an awareness of how the organisation can defend its position there. It means executives must understand their organisation's own digital frontier and the associated risks their organisation faces.

An ***information asset*** is information of value to an organisation while conducting business. The information may be owned by the organisation—for example, customer lists—or it may be information placed under the custodianship of the organisation 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, 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 to be classified as assets.

Eliminating all threats to an organisation's digital assets (and the vulnerabilities that affect them) 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 digital 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 as well as repairing breaches. The work is cyclical and continual, and to engage in it effectively, executive management must know what information assets are at risk, the organisation's current digital security requirements, and its current digital security capabilities. Following a three-step process of assessing the environment, determining responsibilities, and setting priorities lays the foundation for a practical digital security programme.

Step One: Assessing the Environment

A broad understanding of the organisation's digital information assets and operations is required to determine where an organisation's frontier lies. This knowledge helps the organisation to identify and mitigate risk. Identification of this position involves much more than an organisation's simply knowing the usage of and reliance on its computing resources. Senior management must understand which assets to protect and why. For example:

- What are the operational, strategic, or financial issues or requirements driving the organisation's utilisation and reliance on digital technology?

- What are the capabilities of the current digital security programme?

An organisation's executive management needs to answer a number of questions such as:

- What information is worthy of protection?
- Which information requires greater or lesser level of protection?
- Where is the most important information stored?
- Is it clear which versions of the software are being used and are all the copies licensed?
- How quickly are patches assessed and applied?
- Is the software installed on one server or many? In which office or offices are the servers located?
- Who owns the database, and who determines who is allowed access to the data in it? How frequently are backups taken and where are those backups stored?

These are questions that the IT personnel in an organisation should be able to answer quickly. But do these IT specialists understand the value of the information? Should they? Should IT be the only repository of such information?

Organisations need to be able to identify their assets. This identification will involve the IT department certainly, but it is also an activity that must be understood and undertaken by management at the highest levels. Implementing every high-technology security precaution available cannot prevent unauthorised 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 rigour.

The next priority of the asset identification issue is to understand how an organisation's digital security requirements are determined. Is an organisation bound to comply with statutory regulations, including privacy regulations? Do business partners impose specific technical security configurations on an organisation's external networks? What would be the impact of an unintended release of sensitive or critical information?

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 organisation. 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 organisation 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 nonsensitive information would be sales tax information for a retailer—information that is critical to running the business but is unlikely to compromise the organisation if released.

Every organisation has its own mix of regulatory-, industry-, and internally-driven digital security mandates; therefore, the answers to these questions are key to determining each organisation's digital security requirements.

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 organisations, this right extends to the collection, distribution, and storage of that information.

For today's global organisations, attempting to comply with different (sometimes contradictory) legislation and regulation in different jurisdictions can consume large amounts of time and resource.

Once the critical and/or sensitive information has been identified and the security mandates for protecting those assets are understood, the state of an organisation's existing security capabilities can be considered. What does that organisation's digital security programme look like today? For instance, how is the network monitored for unauthorised 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? How much information resides on mobile laptops or palmtop devices and is it secured? Most importantly, could the models on which the answers are based be considered best-in-class, or even fit-for-purpose?

Step Two: Determining Responsibilities

For almost a decade, 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 organisations about digital security. The results are published as the annual *CSI/FBI Computer Crime and Security Survey.*[1] One of the more chilling recent statistics presented in the survey is that 25 percent of respondents have suffered unauthorised access or misuse in the last 12 months to their World Wide Web site,[2] and out of this portion, 24 percent *did not know* if the incident had come internally or externally.[3] Other countries should not feel complacent. For example, in the United Kingdom, the 2004 DTI survey listed the "worst virus attacks" in 2003.[4] One statistic describes how 72 percent of UK businesses had received infected e-mails or files during 2003.[5] Yet a significant number of organisations update their antivirus software only infrequently.[6] The second step in identifying an organisation's security frontier is to *determine executive management's responsibilities* for defending the organisation's position at the digital frontier.

> The overall objective of IT governance . . . is to understand the issues and the strategic importance of IT, so that the enterprise can sustain its operations and implement the strategies required to extend its activities into the future. IT governance aims at ensuring that expectations of IT are met and IT risks are mitigated.
>
> —*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,[7] 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 organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives."[8] Specifically, with IT now so intrinsic and pervasive within enterprises, governance needs to pay special attention to IT, reviewing how strongly the enterprise relies on IT and how critical IT is for the execution of the business strategy.[9]

In today's global, digitally-linked marketplace, executive management has a fiduciary responsibility to shareholders and business partners as well as a responsibility to its organisation. 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 programme that enables management to determine which risks to accept, which risks to mitigate, and which resources to deploy toward mitigation. Carrying out these responsibilities entails the following:

- Setting the objectives for digital security.
- Allocating resources for a programme to achieve and maintain digital security, including monitoring and measuring the programme 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 programme that establishes goals and standards for an implementation framework.

Step Three: Setting Priorities

When an organisation's information systems fail publicly, for whatever reason, and whether the failure affects its networks, its Web site, or any

other subsystem, more than just information is compromised: Trust is lost at every level and the corporate image suffers. The repercussions may be most strongly felt in 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 organisation's position at the frontier.

Earlier in this chapter, we referred to an organisation's digital security requirements and capabilities, and how best to identify digital information assets. Step three raises the same issues from a business perspective. For instance, what is the real threat to an organisation 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 can be compromised in an attack—shareholder and consumer confidence, brand image, share price, or safety of personnel? What are the options with regard to defence? How fast is fast enough when responding to a breach of security? How much is enough to spend defending an organisation's position at the digital frontier?

Executive management's priorities are found in the answers to such questions. The challenge lies in determining what to do *before* a crisis strikes, and then doing it continuously. This means that the entire organisation must adopt a security mindset. It also requires executive managers to learn more than just the technical terminology of an organisation's digital security programme. They will need at least a basic understanding of what digital security means, what it involves, and what such a programme can and cannot achieve. Delegation of authority to those in the organisation who may not understand the business risk versus the business return is inappropriate and possibly dangerous.

There are many different responses to the questions raised in this chapter and they vary between organisations depending on the industry, the product or products produced, the organisation's reliance on technology, and the type of technology in use. Therefore, different organisations will have different priorities. The goal, however, should be the same—to build a digital security programme.

CHALLENGES AT THE FRONTIER

Information has always possessed an inherent value. Therefore, information security is not a new phenomenon. Evidence suggests that information protection is nearly as old as civilised society. Ancient Egyptians, Greeks, and Romans demonstrated varying degrees of expertise in encryption in an effort to keep sensitive information secret. Although the need to protect information remains the same, the methods of doing so have evolved rapidly in the information age.

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 more difficult to protect than ever before.

Threats and Vulnerabilities

Once an organisation has identified its place at the digital frontier and executive management has defined its responsibilities and priorities for defending that place, it must determine the threats it faces and the vulnerabilities of its current security programme. Both threats and vulnerabilities if realised, can cause extreme damage, yet both can be effectively managed.

Five General Consequences of Threats and Vulnerabilities

1. *Interception:* Data is siphoned from the system.
2. *Interruption:* Networks, Internet access, or data stores are rendered unusable in a denial-of-service attack.
3. *Modification:* Authorisations, access codes, or data are changed.
4. *Fabrication:* False information is inserted into a system.
5. *Destruction:* Data is rendered unusable, for example, through a fire, flood, disintegration of old storage media, or other "acts of nature," or deliberate malicious act.

Threats to an information system arise from both human and nonhuman sources. Human threats can be divided into intentional and unintentional ones. Hackers, disgruntled employees, or others who have malicious motivation represent intentional threats. Those who damage systems accidentally—an employee who accidentally deletes important data, for example—are unintentional ones. Nonhuman threats include acts of nature that have no motivation yet could damage or destroy vast amounts of data.

Vulnerabilities are generally inherent weaknesses in an information system, although some vulnerabilities may result from deliberate acts or omissions. Despite quality control mechanisms, little commercial software reaches the market free from vulnerabilities, and systems developed in-house frequently suffer from the same problems. Potential avenues of attack are discovered almost daily, and such information is freely disseminated amongst the IT community and other interested parties, including potential intruders or hackers.

Common Causes of Information System Vulnerabilities

- 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 of security risks.
- Misunderstandings about security protocols and the need for them.
- Developers under time pressure to deliver.

According to the 2003 CSI/FBI Survey, 92 percent of the survey's respondents had detected computer security breaches within the 12 months preceding the survey, and 75 percent acknowledged financial losses due to those breaches. The 47 percent of respondents that were willing or able to quantify their losses reported an aggregate $201 million worth of damage. The most serious areas of loss were the theft of proprietary information, which totalled $70 million, and denial of service, which totalled $65 million. The highest individual loss due to theft of proprietary information was $35 million; the average loss was

$2.7 million. The highest individual loss due to denial of service was $60 million; the average loss was $1.4 million. 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 organisation's e-mail system—cost those who responded $11 million. Despite a high proportion of antivirus software implementation, viruses and their aftermath were detected by 82 percent of respondents and carried a price tag of $27 million.[10]

As this information shows, the risks are real and the stakes are high. All it takes is one person who doesn't "get it" to cause a security breach; that breach can take vast amounts of time, money, and manpower to fix and can have grave repercussions in the marketplace.

There are obstacles beyond threats and vulnerabilities that present challenges for organisations. Many of these obstacles are the product of misconceptions that 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 responsibility of a specialised security group.
- Security threats and vulnerabilities are unique to high-profile industries or organisations.
- Outsiders compromise information most frequently, and such compromise is often detected and prosecuted.
- Security policies are sufficient to guide operations in a secure manner.
- Security technology will solve security needs.
- Security impairs organisational objectives and serves as a barrier to progress.

An Attack Scenario

Many threats exist on the digital frontier. Unfortunately, many organisations' digital security programmes are geared neither towards identifying these threats and addressing vulnerabilities nor responding

appropriately to mitigate the impact of security incidents when such incidents occur. Consider the following real-world scenario and some of the questions it raises from the perspective of an executive who thought the organisation was secure.

Stage One: Onset and Initial Response

An employee who has been with a major healthcare services organisation for 15 years leaves the organisation under unfavorable 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 as requested and change their passwords; others ignore the request. At this stage in the scenario, several issues have been raised:

- The organisation's policy regarding removing employees from the system when they leave is not being followed, nor is the organisation's policy regarding requiring employees to change passwords on a routine schedule.
- The organisation'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. 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 it appears the ex-employee has gained illicit access to the e-mail system, the potential exists that other Internet applications may also have been compromised, such as the organisation'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 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 organisation's information systems are configured to log activity, others are not. However, even those systems that log information are only recording 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 system 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 organisation 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:

- The decision is made to upgrade the situation from being an "incident" to a "crisis."
- 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 organisation managers; this one contains an agenda. It reveals that for some time she was frustrated by the organisation'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 organisation's environment is. At this point the incident is upgraded in importance again, and activating the organisation's business continuity or disaster recovery plans becomes a consideration.

At this juncture, the scenario could move in several directions. However, the point has been made that the well-being of the organisation has been placed in 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 organisation in any industry at any given time.

Executive-level managers and corporate officers must ask themselves how it would be handled if this happened at their organisation:

- Would the digital security programme currently in place have the resources to find the necessary answers, and could it do so in a timely and organised 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 organisation'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 of 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?
- What if such an attack happens again before the organisation has a new programme in place?