Chapter 1

The Information Security Challenge

Four CEOs were taking a break during a recent American Banking Association (ABA) meeting and struck up a conversation about recent challenges they were facing. Howard related a recent incident caused by the Slammer Worm that made his bank’s 13,000 automated teller machines (ATMs) unavailable to their customers for approximately 24 hours. This worm spread so quickly that his information technology (IT) organization could not react in time. A worm is a self-replicating malicious program that doesn’t require user interaction to spread between computers and across networks. Fast-replicating worms can consume resources, slowing computers and networks to a crawl or crashing them altogether.

Sam could relate to Howard’s woes because someone stole a laptop computer that contained private financial information for thousands of customers from one of his bank’s offices. Sam’s business was lucky and recovered the laptop a few days later; however, his customer service organization spent considerable time contacting these customers and continues to monitor their accounts for possible fraud.

Roger was not so lucky. An eastern European hacker tricked his company’s systems into transferring an estimated $10 million into the hacker’s account. His bank was able to recover the majority of these funds, but the incident did considerable damage to his company’s brand. Charles lamented the damage to his credit card business when hackers sent phony but official-looking emails (a process called “phishing”) to his unsuspecting customers to trick them into disclosing confidential information. These hackers then made illegal charges to the accounts of customers who fell for the scam.
The preceding anecdotes are based upon actual recent security incidents that have occurred in the financial services industry. Information security incidents are not limited to this industry, however. All organizations that conduct portions of their business electronically are potential targets. In April 2003, the Slammer Worm disabled a safety monitoring system at a nuclear power plant for nearly five hours and affected the performance of the plant’s corporate network. A major U.S. computer networking company sued a Chinese rival for theft of intellectual property in January 2003. The company claimed that its rival copied its source code, documentation, and other copyrighted information. Both parties settled 20 months later when the Chinese rival agreed to discontinue selling all products named in the lawsuit.

In December 1999, an online music distributor refused to hand over a $100,000 blackmail payment when a hacker stole the confidential personal information, including credit card numbers, of 350,000 of their customers. The hacker posted the information on the Internet, and the resulting brand damage was severe. Finally, two software companies in the Silicon Valley have been embroiled in a billion dollar lawsuit over the theft of intellectual property that allegedly resulted when executives from one of the companies left to form a competitive company.

A lack of knowledge about information security contributed to these incidents and left these companies vulnerable to exploitation. This book explains how you can avoid the same trap and provides you with the resources and best practices necessary to put the information to good use.

Introduction

Information security is a significant boardroom issue. In today’s world, companies rely on their internal computer systems and the Internet to conduct business and cannot afford to have disruptions to their operations. A security incident can have a wide-ranging negative impact on a company’s revenue streams, customer confidence, and public relations. This dilemma makes information security an essential component to an effective overall business strategy. Establishing an information security program that addresses the risks that your business faces should be a high priority.
Overview

This chapter starts with a historical view of the Internet that provides important and relevant background information for understanding information security. It goes on to describe some of the major information security challenges that you’re likely to face and how they can affect your business. These challenges are important to consider when developing your information security program, and you can turn them into competitive advantages.

Understanding the Internet—A Brief History

What is the Internet? The Internet is a global network of computer networks. Each network might contain thousands of computers that are connected or networked together. The term internet is short for internetwork or interconnected network; when capitalized, the term refers to the global internetwork or Internet, which enables millions of computers to communicate with each other on a daily basis.

The Internet was originally intended to be ubiquitous, and it was assumed that its users knew and trusted each other, which facilitated communication. However, as the popularity of the Internet grew, so did the number of users, which led to the deterioration of the trust model. This phenomenon completely changed the usage of the Internet, because users of the system were now at the mercy of a small number of individuals (who became known as hackers) who had the advanced skills needed to fully understand and manipulate the system. Some members of this newly formed community exploited the network’s wide-open design for personal gain or bragging rights.

The popularity of the Internet continued to grow within the academic and government communities, but it did not extend to enterprises due to the technical skills required to access the system and commercial use restrictions. However, this all changed in the early 1990s with the development of Internet browsers such as Mosaic and Netscape Navigator. These advancements revolutionized the Internet, and now in addition to text, web pages contain graphics, pictures, sound, animation, and even video. The popularity of the Internet grew sharply after the advent of these browsers, as shown in Figure 1-1.
Figure 1-1  Internet growth.

The U.S. government also relaxed and later removed commercial use restrictions, and mainstream businesses started to use the Internet as another medium to communicate with their customers, which has now eclipsed the original objectives of sharing information among academic and government organizations.

Although the openness of the Internet enabled businesses to quickly adopt its technology ecosystem, it also proved to be a great weakness from an information security perspective. The system's original purpose as a means of collaboration between groups of trusted colleagues is no longer practical because the usage has expanded into millions of frequently anonymous users.

Numerous security incidents related to viruses, worms, and other malicious software have occurred since the Morris Worm, which was the first and shut down 10% of the systems on the Internet in 1988. These incidents have become increasingly complex and costly. Table 1-1 provides a brief overview of other major incidents over the past few years.
### Table 1-1

**Major Information Security Incidents**

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Morris Worm</td>
<td>1988</td>
<td>■ Stopped 10% of computers connected to Internet</td>
</tr>
<tr>
<td>Melissa Virus</td>
<td>May 1999</td>
<td>■ 100,000 computers in one week</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ $1.5 billion impact</td>
</tr>
<tr>
<td>Explorer Virus</td>
<td>June 1999</td>
<td>■ $1.1 billion impact</td>
</tr>
<tr>
<td>Love Bug Virus (I Love You Virus)</td>
<td>May 2000</td>
<td>■ $8.75 billion impact</td>
</tr>
<tr>
<td>Sircam Virus</td>
<td>July 2001</td>
<td>■ 2.3 million computers infected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ $1.25 billion impact</td>
</tr>
<tr>
<td>Code Red Worm</td>
<td>July 2001</td>
<td>■ 359,000 computers infected in less than 14 hours</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ $2.75 billion impact</td>
</tr>
<tr>
<td>Nimda Worm</td>
<td>Sept. 2001</td>
<td>■ 160,000 computers infected at peak</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ $1.5 billion impact</td>
</tr>
<tr>
<td>Klez</td>
<td>2002</td>
<td>■ $750 million impact</td>
</tr>
<tr>
<td>BugBear</td>
<td>2002</td>
<td>■ $500 million impact</td>
</tr>
<tr>
<td>Badtrands</td>
<td>2002</td>
<td>■ $400 million impact</td>
</tr>
<tr>
<td>Sapphire/Slammer Worm</td>
<td>Jan. 2003</td>
<td>■ Infected 90% of vulnerable hosts in just 10 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 75,000 hosts infected at peak</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ $1.5 billion impact</td>
</tr>
<tr>
<td>Blaster</td>
<td>2003</td>
<td>■ $750 million impact</td>
</tr>
<tr>
<td>Nachi</td>
<td>2003</td>
<td>■ $500 million impact</td>
</tr>
<tr>
<td>SoBig.F</td>
<td>2003</td>
<td>■ $2.5 billion impact</td>
</tr>
<tr>
<td>MyDoom Worm</td>
<td>Jan. 2004</td>
<td>■ Fastest spreading mass-mailer worm to date</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 100,000 instances of the worm intercepted per hour</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ More than $4.0 billion impact</td>
</tr>
</tbody>
</table>

*continues*
The Internet has grown from just a few thousand users in 1983 to more than 800 million users worldwide in 2004. It provides a vital online channel to conduct business with existing and potential customers. However, despite this huge upside, the Internet poses significant security risks that businesses ignore or underestimate at their own peril. The following section describes the major information security challenges to businesses today.

**Six Significant Information Security Challenges**

Executives need to understand and address six significant challenges, which are listed here and reviewed in detail in the following sections:

- E-commerce requirements
- Information security attacks
- Immature information security market
- Information security staff shortage
- Government legislation and industry regulations
- Mobile workforce and wireless computing

**Electronic Commerce**

The Internet has created an important channel for conducting business called electronic commerce (e-commerce). This channel provides many new ways for
Six Significant Information Security Challenges

businesses to offer products and services to their customers. In the past, the ability to connect with millions of customers 24 hours a day, 7 days a week was only possible for the largest corporations. Now even a company with limited resources can compete with larger rivals by offering products and services through the Internet with only a modest investment. E-commerce services are quite appealing to consumers who do not want to spend their limited free time in traditional retail stores constrained by normal business hours of operation, unfriendly staff, and long checkout lines. Executives must understand how to leverage this new channel of electronic commerce while managing the associated risks.

Companies now rely on the Internet to offer products and services according to their customer’s buying preferences. The Internet is no longer an optional sales method but rather a vital distribution channel that a business cannot ignore. Figure 1-2 provides a summary of commerce conducted electronically in 2002.

Figure 1-2  Growth in electronic commerce.

Pioneering companies such as eBay and Amazon have revolutionized the easy purchase of products through the Internet. Not only is it easy for customers to purchase their products, but also companies have innovated the
use of concepts such as “personalization” to create unique relationships with individual customers. Using personalization, companies are able to identify their online customers by name, offer products based upon previous buying habits, and safely store home address information to make purchasing online much quicker. These strategies have enabled successful e-commerce companies to create a positive shopping experience without the overhead associated with traditional retail stores.

Retail securities is another industry that has been transformed as a result of the Internet. In the past, a stockbroker might charge a few hundred dollars to trade a thousand shares of stock. Now a consumer can use an online brokerage firm and complete the same trade for less than twenty dollars. This has revolutionized the securities industry by providing a much more cost-effective service to their customers. It has also put a large number of retail stockbrokers out of work.

Along with increased capabilities come some new challenges that businesses must overcome to be successful. For instance:

- Companies are under tremendous pressure to deliver these systems as quickly as possible because being first to market with a new capability can be a great competitive advantage.
- Timely and accurate access to information for employees, customers, and partners is no longer nice to have—it is expected.
- Companies must offer these services in an easy-to-use but completely secure manner because they store confidential information such as home addresses and personal credit card numbers.
- The systems are expected to be available 24 hours a day, 7 days a week because customers expect to be able to access the products and services at their convenience, not the company’s.

These challenges place considerable demands on IT organizations because delivering these e-commerce systems in a timely and secure manner is very difficult. As expectations increase, so do the demands on the systems and technology.
Constant Growth and Complexity of Information Security Attacks

Security incidents that are related to malicious code (worms, viruses, and Trojans) have grown from slightly annoying to significantly damaging to business operations. A computer virus is a piece of malicious code that attaches to or infects executable programs. Unlike worms, viruses rely on users to execute or launch an infected program to replicate or deliver their payloads. A virus’ payload can delete data or damage system files.

A Trojan (named after the Trojan horse in Greek mythology) is a malicious program disguised as something innocuous, often a utility or screensaver. Like viruses, Trojans rely on unsuspecting users to activate them by launching the program to which the Trojan is attached. Trojans have many functions; some delete or steal data, whereas others install backdoors that enable a hacker to take control of a system. Unlike viruses, Trojans do not replicate.

Early computer viruses were often contained to individual users’ systems, resulting in only a small decline in staff productivity for a given day. However, present-day blended threats, such as Code Red and Nimda, present multiple security threats at the same time, causing major disruptions and billions of dollars of damage to enterprises. A blended threat combines different types of malicious code to exploit known security vulnerabilities. Blended threats use the characteristics of worms, viruses, and Trojans to automate attacks, spread without intervention, and attack systems from multiple points. Figure 1-3 puts things in perspective by illustrating the economics of these attacks over the past few years.

![Figure 1-3](image_url)
These attacks now cause losses of billions of dollars each year, so businesses can no longer ignore the problem. The Love Bug Virus in 2000 had an impact of $8.75 billion alone, causing businesses to finally recognize viruses as a significant issue and to begin to broadly implement anti-virus solutions. This work has lowered the losses experienced since that year; however, the impacts continue to be significant.

Theft of proprietary information is also a major risk to information security. When intellectual property (IP) is in an electronic form, it is much easier to steal. If this information is stored on computers connected to the Internet, thieves can potentially steal it from anywhere in the world. According to the 2003 CSI/FBI Computer Crime and Security Survey, theft of IP remains the highest reported loss. Two recent high-profile examples include an operating system product for a major software company and a version of an operating system for a major networking company. The software company theft was from an authorized third party, whereas the networking company appears to have been compromised by an unauthorized intruder. These types of security problems will only get worse as the Internet continues to grow in usage and complexity.

Three major issues have fueled the growth in security incidents: the increased number of vulnerabilities, the labor-intensive processes required to address vulnerabilities, and the complexity of attacks.

Vulnerabilities are holes or weaknesses in systems that a hacker can exploit to attack and compromise a system. For example, a system administrator can forget to limit certain restricted privileges to authorized users only. This would be like giving everyone on your street a key to the front door of your house when you only meant to give one to your family members. Other examples include existing vulnerabilities resulting from defects in computer software. In these situations, the software vendor should have identified and resolved these weaknesses during the testing processes but overlooked them while under pressure to ship new products by a deadline.

The software industry’s solution to these vulnerabilities is to provide fixes in the form of software patches that a company’s staff must apply to “patch” the “hole.” The process of testing these patches and applying them to your environment is labor-intensive. It is often quite difficult to address the highest-level vulnerabilities and the staggering growth of new vulnerabilities.
compounds this problem. Vulnerabilities reported in 2003 grew by 300% from those reported in 2000. Figure 1-4 summarizes the number of CERT reported vulnerabilities over the past few years.

![Figure 1-4](chart.png)

**Figure 1-4** Security vulnerabilities reported.

The complexity of security attacks has greatly increased over the past few years. The early viruses caused individual productivity issues, but they had nowhere near the impact of blended threats such as Code Red or Nimda. As we mentioned earlier, blended threats use a combination of attack vectors—five in the case of Nimda—to spread more rapidly and cause more damage than a simple virus. For example, Code Red infected 350,000 computers in just 14 hours. In January 2003, the Slammer Worm hit the Internet and had an even higher infection rate than Code Red, infecting 75,000 machines in less than 10 minutes of its release.

The fastest-spreading mass-mailing worm to date was MyDoom in January 2004. At the height of the outbreak, more than 100,000 instances of the worm were intercepted per hour. MyDoom relied on people to activate it and enable it to spread. Cleverly disguised as an innocuous text file attachment, unsuspecting users opened the attachment and launched the worm.

The rapid spread of these threats makes it increasingly difficult to respond quickly enough to prevent damage. Figure 1-5 provides a look at the evolution and growing magnitude of these threats over the past few years:
The threats are expected to continue to grow in magnitude, speed, and complexity, making prevention and clean-up even more difficult. These factors contribute to the need for a proactive plan to address information security issues within every company.

Immaturity of the Information Security Market

The information security market is still in its infancy, with few formal standards established for products or services. The best way to characterize this market would be to compare it to the enterprise resource planning (ERP) market in the early 1980s. Companies at that time were purchasing finance, order processing, and manufacturing systems from separate vendors and having their IT staff integrate these products. This was a time-consuming and expensive process because no standards existed, and interoperability between different vendors was poor. The market then matured, and a small number of vendors such as SAP emerged as industry leaders. These leaders provided a complete solution for companies that included all the individual systems as part of their integrated ERP system. They also established the standards for smaller companies offering complementary functionality. Smaller companies either met the industry leader standards or were pushed out of the market.

The information security industry is at a similar stage today, with several companies offering individual solutions such as firewalls that address only a
portion of a company’s security needs. As a result, their customers face the challenge of making all these solutions work together. Only early versions of standards exist, forcing companies to complete multiple installations of “point” solutions that provide individual components of their security systems.

As with the ERP systems, this will change as a small number of vendors emerge as leaders and offer complete solutions that can support the majority of a company’s information security needs. Smaller niche players in the market will integrate their products with these leaders’ standards because their customers will no longer be willing to have their IT staff perform this role. However, until this day comes, the IT staff continues to bear the daunting task of cobbling all these solutions together. They must deploy a constantly expanding list of products and complete the integration work to ensure that these components are working together.

Another significant challenge that IT technicians face is the sheer amount of data they need to absorb to understand and manage the current state of their computing environment. Each product generates alarms, logs, and so on that they must review to determine whether something is wrong. Figure 1-6 provides a graphic overview of this situation.

![Information security hierarchy](image)

**Figure 1-6**  Information security hierarchy.

Security products generate a great deal of data; however, only a small number of problems or “incidents” might be affecting the company. It is difficult for security staff to get an overall picture of the security environment
and put plans in place to address the critical concerns. This is similar to the business challenge in the 1990s when executive information or decision support systems were developed to mine through large volumes of data to determine critical business trends. Several vendors now offer decision support systems to address this issue for business executives. The “holy grail” for the information security industry is to develop similar systems to solve this problem in the security arena.

An additional challenge is the relative low priority that the software industry places on security. Although some leaders in the software industry have announced a new emphasis on security, the majority of the industry has yet to follow this example. They currently focus on making software easy to use and are under tremendous pressure to deliver new products and services, often sacrificing security. This results in the growing number of vulnerabilities. Until the software industry receives more pressure to prioritize security, even at the sacrifice of new features, this situation will continue.

It will take some time for information security vendors to offer mature solutions to protect your business. In the meantime, you must develop strategies to mitigate these risks. The good news is that the security industry is following a similar pattern to other enterprise software industries, so solutions will be forthcoming.

**Shortage of Information Security Staff**

Finding qualified information security staff is a difficult task, which will likely continue to be the case in the near future. Driving the hiring challenge is the immaturity of the solutions from information security vendors, the limited number of qualified staff available, and the unique blend of information security skills required. Business executives will need to invest more in this area to overcome these challenges.

Due to the immature market, lack of standards, and numerous point solutions, training is a problem for security staff. The industry has not had the time to grow the staff necessary for these roles. In addition, the information security challenges keep growing at a rapid pace, constantly expanding the list of technology to be deployed, and the information security staff just can’t keep up. This translates into more time and money to get your staff trained on commercially available products.
According to the only available survey by CSOOnline.com in 2002, only 60% of the companies responding have an employee who is fully dedicated to information security, and only 32% of those individuals hold a senior-level title such as chief information security officer or chief security officer. These are relatively new titles for most, with an average of two and a half years of experience as head of information security. With the increased focus on information security, we can expect these numbers to increase in the near future.

Obtaining the necessary credentials for information security requires considerable training and experience. The Certified Information Systems Security Professionals (CISSP) credential is an internationally accredited certification and requires passing a test on a broad range of information security topics combined with a minimum of four years of work experience. The related System Security Certified Practitioner (SSCP) credential requires one year of experience plus passing an exam.

Certified Information Security Manager (CISM) also requires a minimum number of years of information security experience along with successfully passing a written exam. All these certifications require ongoing annual training as part of their certification, and GIAC requires periodic testing every two years. Security professionals holding these certifications are in high demand, and employers will need to compete to attract them to their companies. Certified Information Systems Auditor (CISA) requires a minimum of five years of work experience before sitting for an exam. SANS Global Information Assurance Certifications (GIAC) requires candidates to submit a practical work assignment as part of their certification. Certified Information Security Manager (CISM) also requires a minimum number of years of experience.

In addition to specific technical training, information security staff members need to develop security enforcement skills that are not part of the traditional IT staff background. The military, intelligence, and law enforcement fields have traditionally conducted training in this area. In some respects, a company’s security policies are similar to “laws” that must be enforced within a company, which requires specialized training. This unique requirement makes it difficult for existing IT staff to transition into information security roles without receiving specialized enforcement training.

Six Significant Information Security Challenges

According to the only available survey by CSOOnline.com in 2002, only 60% of the companies responding have an employee who is fully dedicated to information security, and only 32% of those individuals hold a senior-level title such as chief information security officer or chief security officer. These are relatively new titles for most, with an average of two and a half years of experience as head of information security. With the increased focus on information security, we can expect these numbers to increase in the near future.

Obtaining the necessary credentials for information security requires considerable training and experience. The Certified Information Systems Security Professionals (CISSP) credential is an internationally accredited certification and requires passing a test on a broad range of information security topics combined with a minimum of four years of work experience. The related System Security Certified Practitioner (SSCP) credential requires one year of experience plus passing an exam.

Certified Information Security Manager (CISM) also requires a minimum number of years of information security experience along with successfully passing a written exam. All these certifications require ongoing annual training as part of their certification, and GIAC requires periodic testing every two years. Security professionals holding these certifications are in high demand, and employers will need to compete to attract them to their companies. Certified Information Systems Auditor (CISA) requires a minimum of five years of work experience before sitting for an exam. SANS Global Information Assurance Certifications (GIAC) requires candidates to submit a practical work assignment as part of their certification. Certified Information Security Manager (CISM) also requires a minimum number of years of experience.

In addition to specific technical training, information security staff members need to develop security enforcement skills that are not part of the traditional IT staff background. The military, intelligence, and law enforcement fields have traditionally conducted training in this area. In some respects, a company’s security policies are similar to “laws” that must be enforced within a company, which requires specialized training. This unique requirement makes it difficult for existing IT staff to transition into information security roles without receiving specialized enforcement training.
Chapter 1—The Information Security Challenge

Probably the greatest challenge in this area is finding a leader who has a broad background in the field and who can pull together an effective information security team. Few candidates have been in the information security field for more than a couple of years and have the required blend of technical and security enforcement skills. They also face the leadership challenge of taking inexperienced staff and developing them into effective information security professionals while dealing with ever-increasing security risks. These individuals are rare and in high demand.

Executives will need to consider longer-term strategies to address these needs because finding trained staff is not just a question of money but also of the time necessary to build the team around a limited number of qualified staff.

Government Legislation and Industry Regulations

Recent information security incidents and increased reliance upon the Internet have prompted governments around the world to create additional legislation to regulate the technology ecosystem. This legislation spans broad areas, such as consumer privacy, to specific regulations for industries, such as health care and financial services. Because the Internet is easily accessible from many places in the world, it is important to understand and operate in compliance with these regulations. Companies that adhere to these regulations and thereby offer their customers a safe and secure method for conducting business can differentiate themselves from their competitors.

Privacy is a major issue in electronic commerce due to the high risk of misuse of personal information. Computer systems contain personal information for millions of customers, and if companies do not take the necessary precautions to ensure that this information is safe and secure, their customers can have their identities—including data such as name, address, phone number, and credit card numbers—stolen and sold to the highest bidder on the Internet. Previously, only a highly skilled hacker could break into these systems and access confidential information. This is no longer the case; now a novice can use readily available tools and gain access into these systems if the company does not use the proper safeguards.

This situation has prompted considerable legislation to protect the rights of consumers because their personal information is now much more readily
available in electronic format. The European Data Protection Directive is an important regulation because Europeans take a much stricter view of privacy than the United States.

This directive prohibits the export of personal data such as name, address, and telephone number to countries that do not meet the European Union’s minimum standards for consumer privacy protection. These standards require that no one can sell, rent, or transfer consumer data to a third party without that individual’s explicit permission. This directive applies to customer information but also includes employee information contained in companies’ internal human resource systems.

In May 2000, the Safe Harbor Agreement was enacted for U.S. companies that are regulated by the U.S. Federal Trade Commission (FTC) and have operations in the European Union. This agreement enables these organizations to comply with the European Data Protection Directive by adopting Safe Harbor Agreement Principles.

These principles require controls to ensure that personal information is protected from loss, misuse, unauthorized access, disclosure, and so on as a condition to obtain certification. Companies certified under the Safe Harbor Agreement can obtain permission to transfer data out of the European Union for renewable one-year periods. It is safe to say that other countries will adopt similar legislation for protecting the privacy of consumer information for their respective citizens.

An important consideration for business executives to remember is that laws and regulations are generally enacted on a country-by-country basis and electronic commerce is performed globally. As soon as your business uses the Internet to conduct business, you are doing business on a worldwide basis. This has the tremendous advantages of offering your products and services globally; however, you also need to comply with local regulations. These regulations are by no means consistent, and you could easily find yourself conflicting with one regulation by complying with another. The Safe Harbor Agreement is an example of the U.S. working out an agreement with the European Union to meet their regulations. Other countries will follow similar strategies to ensure that their industries are competitive and that they can operate freely in major markets such as the European Union.
One major challenge is that certain countries do not place a high priority on protection of personal information or intellectual property. They might have more pressing issues, such as food or medicine, and might be unwilling or unable to police individuals who are engaged in activities such as software piracy. These criminals operate freely in these countries without the fear of law enforcement agencies shutting down their operations. These safe havens for cyber criminals pose additional challenges for legitimate businesses that have little legal recourse to combat the illicit activities of software pirates. Unless business executives put strategies in place to protect their intellectual property and customer information, they run the risk of falling victim to these individuals.

Two industry-specific regulations in the U.S. on privacy include the Gramm-Leach-Bliley Act (GLBA) of 2001 and the Health Information Portability & Accountability Act (HIPAA) of 1996. GLBA applies to financial institutions and requires these organizations to put the controls in place to ensure the security and confidentiality of customer information. Examples of this information include names, addresses, phone numbers, bank and credit card numbers, credit history, and social security numbers. The boards of directors for these institutions are responsible for developing effective information security programs to ensure compliance with these regulations and monitoring these programs on an ongoing basis. These institutions must monitor their service providers to ensure they have the necessary controls in place to manage consumer information. Some key provisions of the act include clear disclosure of company’s privacy policy regarding sharing of non-public personal information. They are also required to provide a notice to consumers and give them the opportunity to “opt out” or decline the sharing of their personal information with third parties.

HIPAA proposes to streamline the healthcare industry, reduce fraud, and make it easier for employees to switch jobs even if they have preexisting medical conditions. One of the key objectives is to standardize and automate key administrative and financial transactions that previously were paper-based. HIPAA establishes standard data formats for these transactions and the controls that must be in place to ensure that this information is secure. To ensure the privacy and confidentiality of patient’s medical records, it institutes standards for the privacy of individually identifiable health information.
All companies handling medical data must adhere to HIPAA requirements for privacy—not just companies within the healthcare industry. These organizations will need to review these regulations in detail to ensure that they are in compliance.

The Sarbanes-Oxley Act is a response to the corporate corruption and failure of many companies during the Internet boom and subsequent bust that occurred during the 1999–2002 period. This U.S. law went into effect in July 2002 and is intended to protect investors by improving the accuracy of corporate disclosures. All U.S. public companies must meet financial reporting and certification mandates for all financial statements filed after June 15, 2004. Smaller companies and foreign corporations that are publicly traded in the U.S. market must meet these regulations for any statements filed after April 15, 2005.

The act is divided into 11 titles, and section 404 that addresses internal controls has generated the most concerns. The act calls for severe penalties for non-compliance, including the possibility of criminal prosecution for executives. From an information security perspective, it is difficult to achieve compliance under Sarbanes-Oxley without having an effective information security program to protect your vital financial information. Adequate controls must also be implemented to ensure that only authorized individuals are able to access this information. Change control processes must also be in place to ensure that any changes to your financial systems are implemented in a controlled manner. Finally, you need to have a business resumption program in place to ensure that your organization can continue to operate in the event of a disaster. Access and change control are covered in more detail in later chapters, whereas business resumption is beyond the scope of this book.

California Senate Bill (SB) 1386 went into effect in July 2003 and requires companies that conduct business in California to disclose any breach of security related to personal data. This law applies to both business and government agencies that own or license computerized data containing personal information. Security breaches include unauthorized access of computer data that compromises the confidentiality or integrity of personal information. Personal information includes social security numbers, driver’s license numbers, and account, credit, or debit card numbers. Written or electronic notice must be given to individuals who are affected by this breach of security.
For companies doing business on the Internet, the implications of SB 1386 are far-reaching for information security because many of these businesses have customers in California and are therefore subject to SB 1386. Public notification of these security breaches can be embarrassing to companies and can have a direct impact on their brand and revenue stream. Penalties can be imposed on organizations that do not comply with the notification requirements. These regulations place additional importance on having an effective information security program in place for any company that plans to leverage the Internet to conduct business.

These are just a few examples of government and industry regulations that can affect how a company conducts business electronically. With the growing number of e-commerce security incidents, the number of regulations will continue to grow. When you start conducting business through the Internet, you are operating on a global basis and must conform to laws and regulations in many different countries. It is important to understand these laws and the restrictions that they can pose. Health care and financial services companies must give special consideration because they have specific regulations with which they must comply. Successful business executives will develop strategies that turn these challenges into competitive advantages.

**Mobile Workforce and Wireless Computing**

The arrival of mobile computing devices has had a significant impact on everyday life. Wireless communications liberate employees and consumers from relying on phone lines to communicate. Looking for a phone booth to make a call or going to the office to access email is quickly becoming a fading memory. Information availability and communications have greatly increased due to mobile computing devices. With the convenience of these devices, information security concerns increase because the confidential information stored on them needs to be protected.

In the past, staff members typically used one computer in the office for business purposes and a different one at home for personal use. These lines have blurred considerably over the past few years, with the use of mobile computers now surpassing the number of desktop computers that remain in a home or office. Laptop computers now enable employees to continue
working at any time from any location. Personal computing devices for storing name and address information, phone numbers, and so on are no longer restricted to business professionals because teenagers now keep track of this information using mobile devices. Figure 1-7 provides some insight into current and projected usage of wireless users.

<table>
<thead>
<tr>
<th>Wireless Internet Usage and Projection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year-End</td>
</tr>
<tr>
<td>USA</td>
</tr>
<tr>
<td>Internet users (millions)</td>
</tr>
<tr>
<td>Wireless Internet User Share</td>
</tr>
<tr>
<td>WorldWide</td>
</tr>
<tr>
<td>Internet Users (millions)</td>
</tr>
<tr>
<td>Wireless Internet User Share</td>
</tr>
<tr>
<td>Asia-Pacific</td>
</tr>
<tr>
<td>Internet Users (millions)</td>
</tr>
<tr>
<td>Wireless Internet User Share</td>
</tr>
<tr>
<td>W. Europe</td>
</tr>
<tr>
<td>Internet Users (millions)</td>
</tr>
<tr>
<td>Wireless Internet User Share</td>
</tr>
</tbody>
</table>

Source: Computer Industry Almanac

Figure 1-7  Wireless Internet usage and projections.

The introduction of the 802.11 protocols for wireless local area networking in 1999 has revolutionized the mobile computing industry. The 802.11 protocols are the equivalent of a common "language" that enables these mobile devices to communicate with each other. Wireless adapters that take advantage of the 802.11 protocols are available for mobile devices. In some areas, wireless ISPs have begun offering high-speed Internet access without the need for phone lines or a cable connection. Accessing the Internet, sending email, and logging into the company network is now possible from the home, backyard, or your favorite park.

The challenge from a security perspective is twofold—first, all the protection offered in the company office must now be incorporated on the laptop computer or mobile device, and second, 802.11 protocols have weak security features. When physically in the office, employees can take advantage of the company’s security protection such as firewalls and anti-virus software. These products can be set up to operate in the background, and employees often do not realize that these products continually protect their systems from threats such as computer viruses. When employees leave the office, this
same protection must be included on notebook computers or handheld devices to ensure that they can continue to operate in a safe and secure manner. In addition to the lack of information security tools, mobile devices that might contain valuable intellectual property, customer information, or other sensitive information also run the risk of theft or loss.

New technologies often initially focus on features and functionality at the expense of security to obtain critical mass and adoption. This is the case of 802.11, as individual consumers have initially embraced this technology and are less concerned with someone reading their email or obtaining access to their personal address book. Businesses, on the other hand, cannot take those risks because enterprise systems contain vital company records that could disrupt their operations if divulged to unauthorized parties. Companies must give careful consideration before leveraging wireless technology in mainstream business.

These information security risks include all the mobile devices such as cell phones, personal digital assistants, and so on that contain valuable information. As a result, companies need to ensure that their information security program extends to all devices that frequently leave the office and that are easily lost or stolen. They can no longer count on safely locking computers in the offices when employees go home at night. Wireless communication offers many compelling advantages over traditional wired communications, but controls must be in place to ensure that the company’s most valuable secrets are secure.

Information Security Challenge Summary

The Internet is a powerful tool for businesses today, and it is important to understand the inherit security risks when leveraging this technology. The Internet was based on ubiquitous communications between trusted parties that does not exist today now that the number of users has grown to hundreds of millions. Major challenges exist today that businesses must consider when leveraging the Internet, and this chapter provided some insight into the importance of including information security in your future business strategy.
These risks will not go away, and successful companies will adopt strategies to minimize them and offer unique solutions to their customers. Information security can be used as a strategic differentiator, especially in a global economy that conducts more business electronically. Secure business systems are a value-added selling tool in an increasingly savvy and cautious customer base. It is much better to incorporate some basic information security principles in your business operations rather than delegating these activities to your IT department and hoping that they adequately address them.

**Essential Components for a Successful Information Security Program**

The following 10 areas are essential for your information security program to be effective:

1. Make sure the CEO “owns” the information security program.
2. Assign senior-level staff with responsibility for information security.
3. Establish a cross-functional information security governance board.
4. Establish metrics to manage the program.
5. Implement an ongoing security improvement plan.
6. Conduct an independent review of the information security program.
7. Layer security at gateway, server, and client.
8. Separate your computing environment into “zones.”
9. Start with basics and then improve the program.
10. Consider information security an essential investment for your business.

We will describe these components in more detail in the remaining chapters of this book and provide suggestions on how to incorporate them into your information security program.
**Key Points for This Chapter**

- Information security is a significant boardroom issue that executives need to understand to conduct business electronically.
- Security incidents have grown from minor annoyances to significant issues with billion dollar impacts.
- Electronic commerce has created a new channel for conducting business that relies upon an effective information security program to gain the trust of customers.
- Security incidents will continue to grow in speed, complexity, and business impact.
- The information security market is immature, and complete solutions do not exist today.
- Government and industry legislation will continue to evolve in an effort to protect consumers and enterprises that conduct more of their business electronically.