

INTRODUCTION

Every day, new stories of viruses, hacker attacks, and security gaffes flood the news media. In the first half of 2002, 3,279 new viruses infected computers around the world, according to antivirus software company Sophos.¹ Meanwhile, high-profile denial-of-service attacks against prominent Web sites such as eBay and Yahoo! have prompted Congressional hearings.² Everywhere you look, it seems, the seamy underbelly of the computer world is out to get you. You could spend countless dollars buying the latest technology to defend against every possible attack. But that strategy is always two steps behind. No matter how many attacks you fend off, there's always one that you didn't expect.

Over the past twenty years, I have advised numerous companies and government organizations on information security, and I've seen many of them make grave security mistakes. One company stores and manages sensitive business and financial information for its customers. Given that many of this company's customers compete with each other, this firm went to great lengths to make sure that no one would be able to access a customer's information except for that customer. Unfortunately, all of this company's security efforts focused on protecting against attacks coming in through the front door. The company didn't examine its own back-office operations, which included sending all of the sensitive information from clients to an overseas supplier whose job was to put all of the data into a standard format.

There was no protection for this information while it traveled over the Internet between the company and the overseas supplier, nor were there any security mechanisms to protect the information while it was at the supplier's site.

In another instance, a brokerage firm with operations in more than forty countries decided to upgrade the information security protections for the systems its employees use to perform financial transactions on behalf of clients. This brokerage firm purchased state-of-the-art-technology to identify employees when they logged on and to keep detailed records of every action their employees took. The technology followed the model of using a passport, in which an official checks both that the passport is valid and that it belongs to the person presenting it. The security vendor that sold this authentication technology went to great lengths to make sure the "passports" employees presented while logging on were valid. However, the vendor neglected to make sure a passport actually belonged to the employee presenting it. If this security flaw had not been discovered and fixed before the brokerage firm installed the software, any employee at this firm could, with no hacking skills and with little difficulty, impersonate any other employee at the firm. Once the impersonation began, all of the actions of the rogue employee would have been attributed to someone else.

Both companies thought they were doing the right thing. They took action to fix security problems, but they didn't go far enough. In these and many other situations, the security holes were invisible to the companies, but left them perilously close to disaster.

WHY ADDRESS SECURITY?

Why should businesses address information security, and why is it important to do so in a comprehensive way? One answer is risk management. Attacks on corporate computers and the theft and misuse of corporate information pose risks that responsible businesses need to

assess and manage. Guarding against information security breaches carries the same fiscal responsibility as protecting a company's physical assets.

However, there is another reason why businesses should take a second and harder look at information security: the critical role it plays in transforming the way businesses operate and in opening up new business opportunities. Consider the film industry. Producing a feature film involves massive amounts of sensitive information, from film and soundtrack clips to financing and marketing plans. Individuals working around the globe need access to this information, and it must be shared securely and conveniently. The current practice for distributing "dailies," the results of a day's filming, involves couriers and overnight delivery services. With the right information security protections in place, dailies could be sent instantly over the Internet to everyone who needs them, regardless of their location, resulting in a substantial increase in efficiency and flexibility. This could shorten decision-making time, facilitate collaboration, and compress filming schedules.

Today, most businesses consider information security a reactionary position, not an enabling technology. A flurry of security activity often follows an attack, such as a virus or a Web site crash. Companies also address security to avoid the pain of noncompliance with government regulations. The financial services and health care industries have paid close attention to information security to meet government regulations, since regulators can force a company that doesn't comply to close its doors.

The common theme across all of these approaches is that while they address immediate security concerns, they are defensive tactics that fail to address the larger role information security should play in today's business environment.

Businesses increasingly rely on the secure use and sharing of digital, or computer-based, information to operate competitively and grow. This digital information includes a wide range of business assets, such as engineering diagrams for a new automobile engine, the terms of a

proposed corporate acquisition, or the destination account number for an electronic funds transfer. This dependence on the reliability and security of digital information is not limited to companies born on the Internet, such as online music and bookstores or Internet stock trading firms. Every company that uses computers to manage some part of its business—even if it doesn't use the Internet at all—needs to worry about information security. Even companies that don't have computers in-house need to be concerned, because the security of the digital information managed by companies with whom they do business affects them as well.

WHO SHOULD READ THIS BOOK

This book addresses the needs of businesspeople who recognize the importance of protecting their company's critical information assets. It is designed to help managers understand the powerful relationship between information security and their organization's growth strategy.

Information security isn't just the domain of the information technology (IT) department. Because senior management is responsible for ensuring the ongoing health and success of a company, understanding the impact of information security practices and policies is paramount. Information security also plays a role in developing new products, expanding to new markets, and improving operational efficiency. Businesspeople need to understand the information security protections their future plans need, as well as the future plans information security can enable.

Although this book focuses on the information security issues facing businesses, the concepts and practices discussed here are directly applicable to government and nonprofit organizations as well. All enterprises need to address information security in a comprehensive way, and the processes for doing this are largely the same. The fundamental security issues surrounding the sharing of sensitive information between different companies are the same as those for sharing sensitive information between different government organizations.

THE ROLE OF TRUST

This book introduces a unique approach for developing and implementing a corporate security process. This approach to information security is based on two principles. The first is that any effective corporate security process has to be closely linked to the *specific* business activities and mission of the company. All measures to secure a company's information and systems that are not based on an understanding of what a company does are inherently incomplete because they can only protect against generic attacks on a company's computers.

The second principle is that *trust* is an essential component of all business activities. You need to know what to trust so that a business activity can meet its objective, and you need to know what evidence is required to establish that trust. This has been prudent business practice since the beginning of commerce.

In the early fifteenth century, for example, the Chinese merchant fleet, under the direction of Admiral Zheng He, made extensive trading voyages throughout the East and South China Seas, the Indian Ocean, and the Persian Gulf.³ In order to accomplish their business objectives of increased wealth and influence, government officials and merchants knew that they needed to trust that the contents of their treasure ships were safe from theft or damage. The warships, patrol boats, and tens of thousands of soldiers and sailors that escorted the treasure ships provided the necessary evidence to establish this trust. When undertaking any business activity, you need to understand what must be trusted to accomplish your business objectives, and what it takes to establish this trust. You need a Trust Framework.

The Trust Framework is built on two elements: trust objectives and trust evidence.

- *Trust objectives* are the security attributes of a business activity—for example, a corporate merger or sale of a product—that a businessperson or company must believe are true in order to be confident that the activity can succeed and accomplish its

business objectives. Examples of trust objectives include being sure that a business partner is who he says he is, keeping sensitive business information secret, and having an official record of a business transaction. Trust objectives are the same in the digital and non-digital worlds.

- *Trust evidence* provides the proof necessary for a businessperson or company to believe that the trust objective has been met. In the non-digital world, trust evidence is often obvious. An introduction by a mutual colleague is a common form of trust evidence for establishing the identity of a new business partner. Sending a document via registered mail or a bonded delivery service provides the necessary evidence for keeping sensitive information secret in most cases, and paper receipts provide evidence of completed business transactions. But as business operations move to the digital world, these common forms of evidence disappear.

The role of information security technology within the Trust Framework is to provide the necessary evidence to meet a company's trust objectives in the digital world. It provides the reasons why a businessperson trusts that the partner he has communicated with only via e-mail is who he claims to be, why he trusts that the sensitive document he sent over the Internet won't fall into the hands of a competitor, and why he trusts that the partner can't repudiate an online business transaction after the fact.

This is a significantly different approach to security from one centered on technologies such as firewalls and virus protection. Those technologies focus on securing a company's computers and networks. In contrast, the security process described in this book focuses on the fundamental issue of securing a company's business activities and information. The process includes the use of technologies such as firewalls, but always in the context of a company's business objectives.

The value of the Trust Framework extends beyond its role in helping companies select information security technology. When a company defines its trust objectives for a business activity, it is making an explicit statement about what security means for that activity. By linking its selection of information security technologies and procedures to its trust objectives, a company offers explicit evidence of how it is making a business activity secure.

Only with this information can a business accurately assess and manage the risks associated with its online business activities. Furthermore, only with this information can potential business partners, customers, and government regulators gauge the safety of conducting business with a company. By contrast, knowing that a company has a firewall and uses virus protection doesn't provide any meaningful information about how safe it is to conduct business with that firm over the Internet.

This direct linkage between trust objectives and security technology also provides a quick answer to the question of why a company is spending time and money on an information security solution. If a company can't tie a security solution back to a business trust objective, it probably shouldn't be using that solution.

BUILDING A BETTER CORPORATE SECURITY PROCESS

The structure of this book mirrors the process of evaluating a company's information security requirements and deploying solutions to meet those requirements over time. The first few chapters discuss the initial steps of the corporate security process and traditional approaches to computer security. The middle of the book lays out the Trust Framework and the four main trust objectives, and the information security technologies that provide evidence that those objectives have been met. The last two chapters provide guidance for companies on organizational issues associated with implementing a comprehensive corporate security process, and on using the Trust Framework to

identify and pursue new business opportunities. Appendix B contains a diagram that guides companies through the entire process.

1. Identifying Your Information Assets

The first step in protecting your company's information assets is to identify them. Assets can take the form of electronic versions of paper documents, or data that control automated functions, such as package routing. Once you've identified the assets you want to protect, you need to prioritize them based on their value to your company.

2. Determining Your Current Vulnerabilities

First, look at all the information assets that your existing security solutions allow users to access. Then, assume the role of a hacker and look at all the subversive ways an outsider could gain access to company information. The combination of both perspectives provides a full picture of the current vulnerabilities facing your company's sensitive business information.

3. Protecting Your Computers

Security technologies such as virus protection, intrusion detection, networking monitoring, and firewalls are important, but they don't address the protection of specific corporate information assets. Chapter 3 provides a brief discussion of these technologies and explains how they fit within the overall corporate security process.

4. Developing a Security Process Based on Trust

Look at information security technology in a new light. Determine what your company needs to trust in any given business activity and select information security technologies based on their ability to establish this trust in the digital world.

5. Keeping Information Confidential

The first trust objective addresses the need for a private environment in which to conduct business and the importance of protecting the

confidentiality of sensitive business information. Encryption can provide companies with the privacy and confidentiality they need.

6. Establishing Identity

Without knowing who a company's partners, suppliers, or customers are, virtually all business transactions would be impossible. Chapter 6 explains how companies can create and authenticate digital identities to establish trust in their online partners.

7. Controlling Access in the Digital World

The value a company derives from its information assets depends on the company's ability to deliver information to the right people while preventing the wrong people from accessing it. Chapter 7 covers information security options, such as controlling access by job function or role.

8. Knowing What's Real in Cyberspace

Written documents and signatures have traditionally provided companies with reliable business records. In a digital business environment, these reliable records don't exist. This final trust objective chapter addresses how companies can use security technologies such as auditing and encryption to create reliable electronic records.

9. Putting Your Security Process into Action

Protecting company information assets entails organizational issues as well as technological obstacles. These include getting senior executives to buy in, budgeting, and building a security team. Companies also need to think about how they can incorporate information security awareness into everyday business decisions.

10. Transforming Your Business Through Information Security

Once a company has addressed its current information security requirements, the next step is to explore the new business opportunities it can pursue with the right information security support. The world

today is full of examples of business activities, from online shopping to the distribution of movies to theaters, that information security makes possible. The Trust Framework can help companies identify new opportunities of their own.

An entirely new era of information security is underway. Information security technology appears complex, and the void between a business function, such as selling a product, and a security mechanism, such as encryption, can seem quite large. The good news is that although the pace of technology change continues to increase, the fundamental information security issues facing businesses remain constant. Moreover, businesses were addressing these issues long before computers existed. It all comes down to trust: Determine what needs to be trusted in a business activity, and then make sure that an acceptable basis for that trust exists.