COMPUTER SECURITY FUNDAMENTALS

THIRD EDITION

CHUCK EASTTOM

Computer Security Fundamentals

Third Edition

Chuck Easttom

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

Computer Security Fundamentals, Third Edition

ISBN-13: 978-0-7897-5746-3
ISBN-10: 0-7897-5746-X

Library of Congress control number: 2016940227

Printed in the United States of America

First Printing: May 2016

Executive Editor
Brett Bartow

Acquisitions Editor
Betsy Brown

Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Gill Editorial Services

Indexer
Brad Herriman

Proofreader
Paula Lowell

Technical Editor
Dr. Louay Karadsheh

Publishing Coordinator
Vanessa Evans

Cover Designer
Chuti Prasertsith

Compositor
Mary Sudul

Contents at a Glance

Table of Contents

About the Author

Chuck Easttom is a computer security and forensics expert. He has authored 20 books, including several on computer security, forensics, and cryptography. He holds 6 patents and 40 computer certifications, including many security and forensics certifications. He has conducted training for law enforcement, federal agencies, and friendly foreign governments. He frequently works as an expert witness in computer-related cases. He is also a frequent speaker on computer security topics at a variety of security-related conferences. You can visit his website at www.chuckeasttom.com.

About the Technical Reviewer

Dr. Louay Karadsheh has a Doctorate of Management in information technology from Lawrence Technological University, Southfield, Michigan. His research interest includes cloud computing, information assurance, knowledge management, and risk management. Dr. Karadsheh has published 11 articles in refereed journals and international conference proceedings and has extensive knowledge in operating system, networking, and security. Dr. Karadsheh has provided technical edits/reviews for several major publishing companies, including Pearson and Cengage Learning. He holds CISSP, CEH, CASP, CCSK, CCE, Security+, VCA-C, VCA-DCV, SCNP, Network+, and Mobility+ certifications.

Dedication

This book is dedicated to my wife, Teresa,
who has helped me become who I am.

Acknowledgments

The creation of a book is not a simple process and requires the talents and dedication from many people to make it happen. With this in mind, I would like to thank the folks at Pearson for their commitment to this project.

Specifically, I would like to say thanks to Betsy Brown for overseeing the project and keeping things moving.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Register your copy of *Computer Security Fundamentals* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789757463 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

It has been more than 10 years since the publication of the original edition of this book. A great deal has happened in the world of computer security since that time. This edition is updated to include newer information, updated issues, and revised content.

The real question is: Who is this book for? This book is a guide for any computer-savvy person. That means system administrators who are not security experts or anyone who has a working knowledge of computers and wishes to know more about cyber crime and terrorism could find this book useful. However, the core audience will be students who wish to take a first course in security but may not have a thorough background in computer networks. The book is in textbook format, making it ideal for introductory computer security courses that have no specific prerequisites. That lack of prerequisites means that people outside the normal computer science and computer information systems departments could also avail themselves of a course based on this book. This might be of particular interest to law enforcement officers, criminal justice majors, and even business majors with an interest in computer security.

As was previously mentioned, this book is intended as an introductory computer security book. In addition to the numerous end notes, the appendixes will guide you to a plethora of additional resources. There are also review questions and practice exercises with every chapter. Appendix C contains the answers to the multiple choice questions for your review. Exercises and projects don't have a single answer. They are intended to encourage the reader to explore, so answers will vary.

This book is not a cookbook for hackers. You will see exactly how hackers target a system and get information about it. You will also see step-by-step instructions on how to use some password-cracking utilities and some network-scanning utilities. You will also be given a reasonably in-depth explanation of various hacking attacks. However, you won't see a specific step-by-step recipe for executing an attack.

This book assumes that you are a competent computer user. That means you have used a computer at work and at home, are comfortable with email and web browsers, and know what words like RAM and USB mean. For instructors considering this as a textbook, that means students will have had some basic understanding of PCs but need not have had formal computer courses. For this reason, there is a chapter on basic networking concepts to get you up to speed. For readers with more knowledge, such as system administrators, you will find some chapters of more use to you than others. Feel free to simply skim any chapter that you feel is too elementary for you.

Chapter 7

Industrial Espionage in Cyberspace

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Know what is meant by industrial espionage
- Understand the low-technology methods used to attempt industrial espionage
- Be aware of how spyware is used in espionage
- Know how to protect a system from espionage

Introduction

When you hear the word *espionage*, perhaps you conjure up a number of exciting and glamorous images. Perhaps you have visions of a well-dressed man who drinks martinis, shaken but not stirred, traveling to glamorous locations with equally glamorous travel companions. Or perhaps you envision some exciting covert operation with high-speed car chases and guns blazing in faraway exotic lands. Contrary to popular media portrayals, espionage is often much less exciting than those visions. The ultimate goal of espionage is to obtain information that would not otherwise be made available. Generally, espionage is best done with as little fanfare as possible. Blazing gun battles and glamorous locations tend to be the antithesis of intelligence gathering. Rather, information is the goal. If possible, it is best to obtain that information without the target organization even realizing that its information has been compromised.

Many people assume that such spying is only engaged in by governments, intelligence agencies, and nefarious international organizations, such as Al Qaida or ISIS. While those entities do indeed engage in espionage, they are certainly not the only organizations that do so. The aforementioned organizations desire to acquire information for political and military goals. However, economic goals are also dependent on accurate and often sensitive data. With billions of dollars at stake, private companies can become engaged in industrial espionage as either a target or a perpetrator. What company would not like to know exactly what its competitor is doing? In fact, corporate or economic espionage is on the rise.

Corporate or economic espionage is a growing problem, but it can be difficult to accurately assess just how great a problem it is. Companies that perpetrate corporate espionage do not share the fact that they do it, for obvious reasons. Companies that are victims of such espionage often do not wish to reveal that fact either. Revealing that their security was compromised could have a negative impact on their stock value. It is also possible, in certain cases, that such a breach of security might open the company to liability claims from customers whose data may have been compromised. For these reasons, companies often are hesitant to disclose any industrial espionage activities. Because you will want to protect yourself and your company, it is important that you learn about espionage methods and protections. In the exercises at the end of this chapter, you will run antispyware, key loggers, and screen-capture software so that you are aware of how they work and, hence, will be cognizant of the risks they pose. While we did cover those in previous chapters, we will expand on that in this chapter's exercises.

What Is Industrial Espionage?

Industrial espionage is simply the use of spying techniques to find out key information that is of economic value. Such data might include details on a competitor's new project, a list of a competitor's clients, research data, or any information that might give the spying organization an economic advantage. While the rationale for corporate espionage is different from military espionage, corporate techniques are often the same as those methods employed by intelligence agencies and can include electronic monitoring, photocopying files, or compromising a member of the target organization. Not only does economic espionage use the same techniques as intelligence agencies, but it often also uses the same people. There have been a number of incidents in which former intelligence agents were found working in corporate espionage. When such individuals bring their skills and training to the world of corporate espionage, the situation becomes much more difficult for computer security experts.

In Practice

Leaving with Sensitive Data

While various computer experts and government agencies attempt to estimate the impact and spread of corporate espionage, its very nature makes accurate estimates impossible. Not only do the perpetrators not wish to disclose their crimes, but often the victims will not disclose the event either. However, anecdotal evidence would suggest that the most common form of espionage is simply an employee who quits, takes a job with another firm, and leaves with sensitive data. In many cases, these employees choose data that is readily available within the company and, as such, the data is considered a "gray area" as to its confidentiality. For example, a salesperson may leave with a printout of contacts and customers so that he can solicit them on behalf of the next employer. It is critical that you have a very well-worded nondisclosure and noncompete agreement with all employees. It is best to solicit the services of an employment attorney to draw up this agreement. Additionally, you might consider limiting an employee's access to data prior to terminating his employment. You should also conduct exit interviews and consider confiscating items such as company phone books, which may at first seem insignificant but which could contain data useful to another company. It is also the case that thumb drives, smart phones, and other technologies provide a method for taking data out of a company. Some companies restrict the use of these devices.

Information as an Asset

Many people are used to viewing tangible objects as assets but have difficulty appreciating how mere information can be a real asset. Companies spend billions of dollars every year on research and development. The discovered information is worth at least the amount of resources taken to derive the information plus the economic gain produced by the information. For example, if a company spends $200,000 researching a process that will in turn generate $1 million in revenue, then that data is worth at least $1.2 million. You can think of this economic gain as a simple equation:

```
VI (value of information) = C (cost to produce) + VG (value gained)
```

While some people are not yet fully cognizant of the concept, data does indeed represent a valuable asset. When we speak of the "information age" or our "information-based economy," it is important to realize that these terms are not just buzzwords. Information is a real commodity. It is as much an economic asset as any other item in the company's possession. In fact, it is most often the case that the data residing on a company's computer is worth far more than the hardware and software of the computer system itself. It is certainly the case that the data is much more difficult to replace than the computer hardware and software.

To help you truly appreciate the concept of information as a commodity, consider the process of earning a college degree. You spend four years sitting in various classrooms. You pay a significant amount of money for the privilege of sitting in a room and listening to someone speak at length on

some topic. At the end of the four years, the only tangible product you receive is a single piece of paper. Surely you can get a piece of paper for far less cost and with much less effort. What you actually paid for was the information you received. The same is true of the value of many professions. Doctors, attorneys, engineers, consultants, managers, and so forth all are consulted for their expert information. Information itself is the valuable commodity.

The data stored in computer systems has a high value for two reasons. First, there is a great deal of time and effort that goes into creating and analyzing the data. If you spend six months with a team of five people gathering and analyzing information, then that information is worth at least an amount equal to the salaries and benefits of those people for that length of time. Second, data often has intrinsic value, apart from the time and effort spent acquiring those facts. If the facts are about a proprietary process, invention, or algorithm, its value is obvious. However, any data that might provide a competitive edge is inherently valuable. For example, insurance companies frequently employ teams of statisticians and actuaries who use the latest technology to try to predict the risks associated with any given group of potential insureds. The resulting statistical information might be quite valuable to a competing insurance company. Even a customer contact list has a certain inherent value.

Thus, as you work in the computer security field, always keep in mind that any data that might have economic value is an asset to your organization and that such data provides an attractive target for any competitors who may not have ethical inhibitions against using espionage. If your company management thinks that this threat is not real, then they are very much mistaken. Any company is a potential victim of corporate espionage. You should take steps to protect your valuable information—and the first critical step in this process is asset identification.

Asset identification is the process of listing the assets that you believe support your organization. This list should include things that impact direct day-to-day operations as well as those that are tied to your company's services or products. The CERT website (http://people.tuke.sk/dezider.guspan/security/___bezpecnost%20OCTAVE%20CERT/Tutorial%20Workbook%20-tutorial-workbook.pdf) offers a very useful worksheet that you can use to itemize the assets in your organization. This workbook also offers a number of other useful worksheets for assuring information security within your organization. As the table of contents in Figure 7.1 shows, this workbook is also a tutorial that steps you through all the information security considerations.

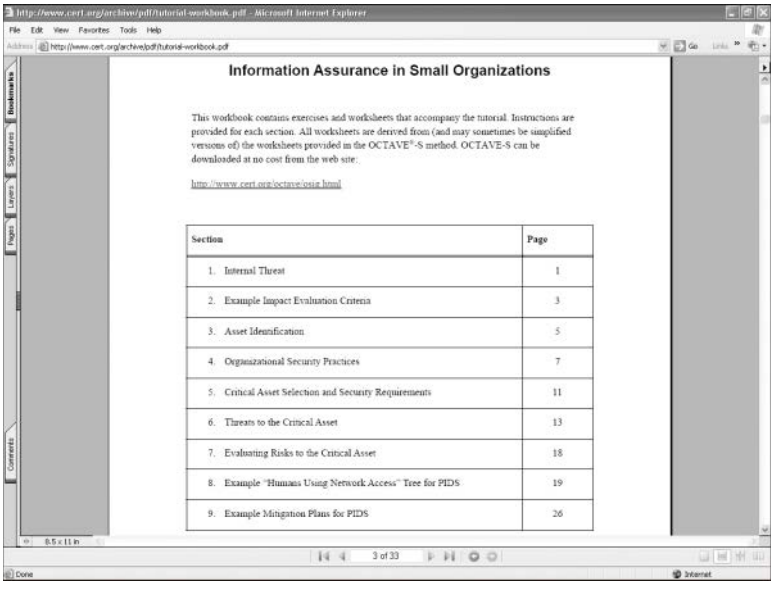

FIGURE 7.1 Table of contents from the CERT Information Assurance in Small Organizations workbook.

Table 7.1 is a variation on the worksheet provided by CERT. Armed with this table and based on your knowledge and experience with the company, you can complete your asset identification following the steps outlined below.

TABLE 7.1 Asset Identification Worksheet

Information	Systems	Services and Applications	Other Assets	

1. In the first column of the table, list the information assets. You should list the types of information used by people in your company—the information people need to do their jobs. Examples are product designs, software programs, system designs, documentation, customer orders, and personnel data.

2. For each entry in the Information column, fill in the names of the systems on which the information resides. In each case, ask yourself which systems people need to perform their jobs.
3. For each entry in the Information column, fill in the names of the related applications and services. In each case, ask yourself what applications or services are needed for individuals to perform their jobs.
4. In the last column, list any other assets that may or may not be directly related to the other three columns. Examples are databases with customer information, systems used in production, word processors used to produce documentation, compilers used by programmers, and human resources systems.

Once you complete the proceeding steps and fill out the Asset Identification worksheet, you will have a good understanding of the critical assets for your organization. With this information, you will know how best to devote your defensive efforts. Some specific protective steps will be examined later in this chapter.

Real-World Examples of Industrial Espionage

Now that you have been introduced to the concept of corporate espionage, let's look at five actual cases. These case studies are of real-world espionage found in various news sources. This section should give you an idea of what types of espionage activities actually occur. Note that while some of these cases are a bit old, they do illustrate the way industrial espionage is done. And it is frequently the case that details of an industrial espionage incident do not emerge until many years later, if at all.

Example 1: Houston Astros

In 2015 the Houston Astros baseball team's scouting and team information database was stolen. It is alleged that it was stolen by members of the St. Louis Cardinals. The Houston Astros have a proprietary internal computer system they named Ground Control. It has notes on players and potential trading of players.

The Astros general manager, Jeff Luhnow, had previously worked for the Cardinals, and when he came to work for the Astros, he also brought along some of his staff. Initial reports are that either Mr. Luhnow or one of his staff used a password similar to what he had used with the Cardinals. This allowed someone associated with the Cardinals to guess the password and access the Houston Astros database.

Example 2: University Trade Secrets

In May 2015, Professor Hao Zhang of Tianjin University and five other individuals were arrested and charged with stealing trade secrets for use by universities controlled by the Chinese government. The secrets stolen included research and development on thin-film bulk acoustic resonator (FBAR) technology.

The details of FBAR technology are not important for our discussion of this case of industrial espionage, but I will provide you with a brief description: It is essentially a device that has material located between two electrodes and acoustically isolated from the medium it is in. This is commonly used as a radio frequency filter in cell phones.

Example 3: VIA Technology

VIA Technology actually provides two examples of industrial espionage. In the first instance, the chief executive officer (CEO) of the firm, which was based in Taipei, was indicted for copyright infringement for allegedly stealing technology from one of his own customers, a networking company called D-Link (Network World Fusion, 2003).

According to the allegations, VIA engineer Jeremy Chang left VIA to work for D-Link. For several months while at D-Link, Chang continued to receive a paycheck from VIA. Then he promptly resigned from D-Link and returned to VIA. Once Chang rejoined VIA, a D-Link document that detailed one of its simulation programs for testing integrated circuits was posted to an FTP server owned by VIA.

The prosecutors allege that Chang continued to receive a check from VIA because he had never really resigned. They allege that Chang was in fact a "plant" sent to D-Link to acquire D-Link's technology for VIA. VIA maintains that his continuation to receive a check was simply an oversight, and Chang denies that he posted the document in question. Whatever the truth of the case, it should make any employer think twice about hiring decisions and nondisclosure agreements.

To make matters worse for VIA, another company accused VIA of stealing code for its optical readers. In both cases, the story of the possible theft of technology alone has had a negative impact on the stock value of both companies.

Example 4: General Motors

In 1993, General Motors (GM) and one of its partners began to investigate a former executive, Inaki Lopez. GM alleged that Lopez and seven other former GM employees had transferred GM proprietary information to Volkswagen (VW) in Germany via GM's own network (Brinks et al., 2003). The information allegedly stolen included component price data, proprietary construction plans, internal cost calculations, and a purchasing list.

In 1996, GM followed up the ongoing criminal investigation with civil litigation against Lopez, VW, and the other employees. In November 1996, GM expanded its legal battle by invoking the various Racketeer Influenced and Corrupt Organizations Act (RICO) statutes, originally intended to be used against organized crime conspiracies (*Economist,* 1996). By May 2000, a federal grand jury indicted Lopez on six counts related to fraud and racketeering. As of this writing, the case is not resolved (*USA Today,* 2000). At the time Lopez was indicted, he was residing in Spain, and the U.S. Justice Department was negotiating for his extradition. Thus, you can see that corporate espionage is neither new nor restricted to technology companies.

Example 5: Bloomberg, Inc.

According to the *American Bar Association Journal* (2003), in August 2003, Oleg Zezev, a 29-year-old PC technician from Kazakhstan, broke into the Bloomberg Inc. computer system and used the alias Alex to obtain information and then blackmail the firm.

Zezev entered Bloomberg's computer system and accessed various accounts, including Michael Bloomberg's (CEO and founder of Bloomberg L.P.) personal account as well as accounts for other Bloomberg employees and customers. Zezev copied information from these accounts, including email inbox screens, Michael Bloomberg's credit card numbers, and screens relating to the internal functions of Bloomberg. He also copied internal information that was only accessible by Bloomberg employees.

Zezev then threatened to expose the data he had stolen to the public and, in essence, tell everyone exactly how he had broken into Bloomberg's network unless he received $200,000.

After deliberating for less than six hours, the jury in the U.S. District Court in Manhattan found the perpetrator guilty of all four charges: conspiracy, attempted extortion, sending threatening electronic messages, and computer intrusion. Although this is not industrial espionage in the classic sense, it does illustrate the compromising situations in which a company and its employees can be placed when security is breached.

Example 6: Interactive Television Technologies, Inc.

On August 13, 1998, someone broke into the computer systems of Interactive Television Technologies, Inc. and stole the data for a project the company was working on (Secure Telecom, 1998). That project involved four years of intense research and a substantial financial investment. The product was to be a way whereby anyone with a television could have Internet access via the Web. This product, code named "Butler," would have been worth a substantial amount to its inventors. However, with all the research material stolen, it was only a matter of time before several other companies came out with competing products, thus preventing Interactive Television Technologies from pursuing a patent.

To date, no arrests have been made and no leads are available in this case. This situation was a case of very skillful hackers breaking into a computer system and taking exactly what they needed. One can only speculate about their motives. They may well have sold the research data to competitors of Interactive Television Technologies, or they may have simply put the data out in the open via the Internet. Whatever the motives or profits for the perpetrators, the outcome for the victim company was catastrophic.

Trends in Industrial Espionage

While the cases just discussed range over a number of years, the problem is not abating. In fact, according to a CNN report, 2015 saw a 53% increase in cases of industrial espionage. The FBI conducted a survey of 165 companies and found that half of those companies had been the victim of industrial espionage of some type. A significant number of industrial espionage cases involve insider threats.

Industrial Espionage and You

These cases notwithstanding, most companies will deny involvement in anything that even hints at espionage. However, not all companies are quite so shy about the issue. Larry Ellison, CEO of Oracle Corporation, has openly defended his decision to hire private investigators to sift through Microsoft garbage in an attempt to garner information (CNET News, 2001). Clearly, espionage is no longer a problem just for governments and defense contractors. It is a very real concern in the modern business world. The savvy computer security professional will be aware of this concern and will take the appropriate proactive steps.

How Does Espionage Occur?

There are two ways that espionage can occur. An easy, low-technology avenue would be for current or former employees to simply take the data or for someone to use social engineering methods (discussed in Chapter 3, "Cyber Stalking, Fraud, and Abuse") to extract data from unsuspecting company employees. The second, more technology-oriented method is for the individuals to use spyware, which includes the use of cookies and key loggers. There are other technological methods we will discuss.

Low-Tech Industrial Espionage

Corporate espionage can occur without the benefit of computers or the Internet. Disgruntled former (or current) employees can copy sensitive documents, divulge corporate strategies and plans, or perhaps reveal sensitive information. In fact, whether the method used is technological or not, disgruntled employees are the single greatest security risk to any organization. A corporate spy need not hack into a system in order to obtain sensitive and confidential information if an employee is willing to simply hand over the information. Just as with military and political espionage, the motives for the employee to divulge the information vary. Some engage in such acts for obvious financial gains. Others may elect to reveal company secrets merely because they are angry over some injustice (real or imagined). Whatever the motive, any organization has to be cognizant of the fact that it has any number of employees who may be unhappy with some situation and have the potential to divulge confidential information.

Certainly, one can obtain information without the benefit of modern technology; however, computer technology (and various computer-related tactics) can certainly assist in corporate espionage, even if only in a peripheral manner. Some incidents of industrial espionage are conducted with technology that requires little skill on the part of the perpetrator, as illustrated in Figures 7.2 and 7.3. This technology can include using universal serial bus (USB) flash drives, compact discs (CDs), or other portable media to take information out of the organization. Even disgruntled employees who wish to undermine the company or make a profit for themselves will find it easier to burn a wealth of data onto a CD and carry that out in their coat pocket rather than attempt to photocopy thousands of documents and smuggle them out. And the new USB flash drives, smaller than your average key chain, are a dream come true for corporate spies. These drives can plug into any USB port and store a tremendous amount of data. As of this writing, one can easily purchase small portable devices capable of holding 2 terabytes or more of data.

FIGURE 7.2 Low-tech espionage is easy.

FIGURE 7.3 Low-tech espionage is portable.

While information can be taken from your company without overt hacking of the system, you should keep in mind that if your system is unsecure, it is entirely possible that an outside party would compromise your system and obtain that information without an employee as an accomplice. In addition to these methods, there are other low-tech, or virtually "no-tech," methods used to extract information. *Social engineering*, which was discussed at length in Chapter 3, is the process of talking a person into giving up information she otherwise would not divulge. This technique can be applied to industrial espionage in a number of ways.

The first and most obvious use of social engineering in industrial espionage is in direct conversation in which the perpetrator attempts to get the targeted employee to reveal sensitive data. As illustrated in Figure 7.4, employees will often inadvertently divulge information to a supplier, vendor, or salesperson without thinking the information is important or that it could be given to anyone. This involves simply trying to get the target to talk more than they should. In 2009, there was a widely publicized case of a Russian spy ring working in the United States. One of their tactics was simply to befriend key employees in target organizations and, through ongoing conversations, slowly elicit key data.

Another interesting way of using social engineering would be via email. In very large organizations, one cannot know every member. This loophole allows the clever industrial spy to send an email message claiming to come from some other department and perhaps simply asking for sensitive data. A corporate spy might, for example, forge an email to appear to be coming from the legal office of the target company requesting an executive summary of some research project.

FIGURE 7.4 Social engineering used as low-tech espionage.

Computer security expert Andrew Briney (Information Security, 2003) places people as the number-one issue in computer security.

Spyware Used in Industrial Espionage

Clearly, any software that can monitor activities on a computer can be used in industrial espionage. *Security IT World,* an online e-zine, featured an article in its October 2003 issue that dealt with the fact that monitoring a computer is an easy thing to do in the twenty-first century. The problem still persists to this day, with many security experts stating that spyware is at least as widespread as viruses. One method to accomplish monitoring is via spyware, which we discussed in detail in Chapter 5, "Malware." Clearly, software or hardware that logs key strokes or takes screenshots would be most advantageous to the industrial spy.

The application of this type of software to espionage is obvious. A spy could get screenshots of sensitive documents, capture logon information for databases, or in fact capture a sensitive document as it is being typed. Any of these methods would give a spy unfettered access to all data that is processed on a machine that contains spyware.

Steganography Used in Industrial Espionage

Steganography is a different way of keeping messages secret. Rather than hide them through encryption, it protects communication via obscuring them. Messages are hidden within images. And in some cases other images are hidden within images. The word *steganography* comes from the Greek *steganos*, meaning covered or secret, and *graphy*, meaning writing or drawing. There are several technical means to accomplish this, but the most common is to conceal the data in the least significant bits of an image file. However, data can be concealed in any sort of digital file.

It should also be noted that historically there have been nontechnical means of hiding messages. A few notable examples include the following:

- The ancient Chinese wrapped notes in wax and swallowed them for transport.
- In ancient Greece a messenger's head might be shaved, a message written on his head, and then his hair was allowed to grow back.
- In 1518, Johannes Trithmeus wrote a book on cryptography and described a technique where a message was hidden by having each letter taken as a word from a specific column.

You might think that steganography requires a great deal of technical knowledge to accomplish; however, there are many software packages available that will perform the steganography for you. Quick Stego and Invisible Secrets are two very easy-to-use software tools that will do steganography for you. MP3Stego is a free tool that hides data inside MP4 files. These are just a few of the tools that one can find on the Internet. The widespread availability of cheap or free tools that are easy to use makes steganography a greater threat to any organization.

Phone Taps and Bugs

Of course, there is always the possibility of using phone taps. A phone tap is simply the process of tying into the phone line at some point and intercepting calls. This is often done at some utility location inside the building one wishes to tap. Obviously, this sort of attack requires the attacker to enter on or near the premises, compromise phone equipment, and have the skill to tap into the phone line.

Protecting Against Industrial Espionage

By now, you are aware that there are many ways that your organization's valuable information assets can be compromised. The question thus becomes this: What steps can you take to alleviate the danger? Note that I said "alleviate" the danger. There is nothing you can do to make any system, any information, or any person totally secure. Totally unbreakable security is simply a myth. The best you can do is work to achieve a level of security that makes the effort required to get information more costly than the value of the information.

One obvious protection is to employ antispyware software. As was mentioned earlier in this book, many antivirus programs also have antispyware capabilities. This software, coupled with other security measures such as firewalls and intrusion detection software (both examined in Chapter 9, "Computer Security Technology"), should drastically reduce the chance that an outside party will compromise your organization's data. Furthermore, implementing organizational policies (also discussed in Chapter 9) that help guide employees on safely using computer and Internet resources will make your system relatively secure. If you add to your protection arsenal the strategy of encrypting all transmissions, your system will be as secure as you can reasonably make it. (Chapter 8, "Encryption, is devoted to encryption.) However, all of these techniques (firewalls, company policies, antispyware, encryption, and so forth) will only help in cases in which the employee is not the spy. What do you do to ameliorate the danger of employees intentionally stealing or compromising information? Actually, there are several courses of action any organization can take to lessen risks due to internal espionage. Here are 12 steps you can use:

1. Always use all reasonable network security: firewalls, intrusion detection software, antispyware, patching and updating the operating system, and proper usage policies.
2. Give the personnel of the company access to only the data that they absolutely need to perform their jobs. This concept is referred to as *least privileges*. The employees are given the minimum privileges necessary to perform their job tasks. Use a need-to-know approach. One does not want to stifle discussion or exchange of ideas, but sensitive data must be treated with great care.
3. If possible, set up a system for those employees with access to the most sensitive data in which there is a rotation or a separation of duties. In this way, no one employee has access and control over all critical data at one time.
4. Limit the number of portable storage media in the organization (such as CD burners, and flash drives) and control access to these media. Log every use of such media and what was stored.

Some organizations have even prohibited cell phones because many phones allow the user to photograph items and send the pictures electronically.

5. Do not allow employees to take documents/media home. Bringing materials home may indicate a very dedicated employee working on her own time or a corporate spy copying important documents and information.
6. Shred documents and melt old disks/tape backups/CDs. A resourceful spy can often find a great deal of information in the garbage. If any storage media is disposed of, it should be completely wiped. Degaussing is a good technique for hard drives and USB drives.
7. Do employee background checks. You must be able to trust your employees, and you can only do this with a thorough background check. Do not rely on "gut feelings." Give particular attention to information technology (IT) personnel who will, by the nature of their jobs, have a greater access to a wider variety of data. This scrutiny is most important with positions such as database administrators, network administrators, and network security specialists.
8. When any employee leaves the company, scan the employee's PC carefully. Look for signs that inappropriate data was kept on that machine. If you have any reason to suspect inappropriate usage, then store the machine for evidence in subsequent legal proceedings.
9. Keep all tape backups, sensitive documents, and other media under lock and key, with limited access to them.
10. If portable computers are used, then encrypt the hard drives. Encryption prevents a thief from extracting useable data from a stolen laptop. There are a number of products on the market that accomplish this encryption, including the following:
    - TrueCrypt (see Figure 7.5) is one example of a free tool for encrypting drives, folders, or partitions. The tool is remarkably easy to use and can be found at www.truecrypt.org/. There are several other similar tools; most are low cost or free.
    - Microsoft Windows includes two types of encryption. Windows 7 Enterprise or Ultimate edition includes BitLocker for encrypting entire hard drives. BitLocker is also available on later versions of Windows (8, 8.1, 10). And all versions of Windows since Windows 2000 have included Encrypted File System for encrypting specific files or folders (see Figure 7.6).
    - This list is not exhaustive; therefore, it is highly recommended that you carefully review a variety of encryption products before making a selection.
11. Have all employees with access to any sensitive information sign nondisclosure agreements. Such agreements give you, the employer, a recourse should an ex-employee divulge sensitive data. It is amazing how many employers do not bother with this rather simple protection.

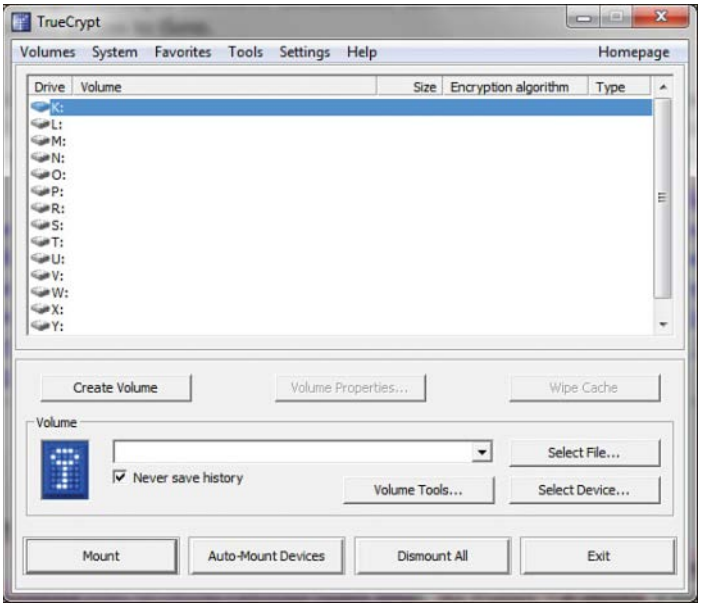

FIGURE 7.5 TrueCrypt.

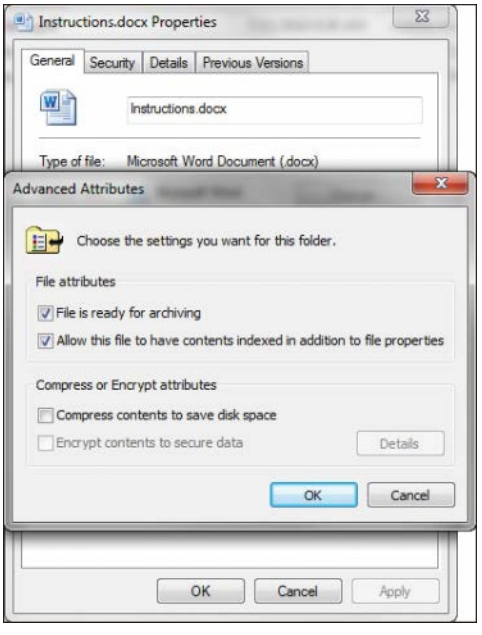

FIGURE 7.6 Windows EFS.

12. Have security awareness sessions. Clearly, employee education is one of the most important things you can do. An organization should have some method for routinely advising employees about security issues. An excellent way to do that is to have an intranet site that has security bulletins posted to it. It is also a good idea to have periodic training sessions for employees. These need not be lengthy or in depth. Most nontechnical employees only need an introduction to security concepts.

Unfortunately, following these simple rules will not make you totally immune to corporate espionage. However, using these strategies will make any such attempts much more difficult for any perpetrator; thus, you will improve your organization's data security.

Industrial Espionage Act

The Industrial Espionage Act of 1996 was the first U.S. law to criminalize theft of commercial trade secrets. This law provides for significant penalties for violators. Quoting from the actual law:[1]

> (a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret, knowingly—
>
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in paragraphs (1) through (3); or
>
> (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

Spear Phishing

Phishing, as you know, is the process of attempting to get personal information from a target in order to steal the target's identity or compromise the target's system. A common technique is to send out a mass email that is designed to entice recipients into clicking on a link that purports to be some financial institution's website but is actually a phishing website.

1. http://fas.org/irp/congress/1996_rpt/s104359.htm

Spear phishing is using the same technology in a targeted manner. For example, if an attacker wanted to get into the servers at a defense contractor, he might craft email and phishing websites specifically to target software and network engineers at that company. The emails might be made to appear of interest to that specific subgroup of people. Or the attacker might even take the time to learn personal details of a few of these individuals and target them specifically. This technique has been used against executives at various companies. In 2010 and 2011, this problem began to grow significantly.

This has since been expanded even more into the process of whaling. *Whaling* attempts to compromise information regarding a specific, but highly valuable, employee. It uses the same phishing techniques, but highly customized to increase the chances that the single individual target will be fooled and actually respond to the phishing attempt.

Summary

A number of conclusions can be drawn from the examination of industrial espionage. The first conclusion: It does indeed occur. The case studies clearly demonstrate that industrial espionage is not some exotic fantasy dreamed up by paranoid security experts. It is an unfortunate, but quite real, aspect of modern business. If your firm's management chooses to ignore these dangers, then they do so at their own peril.

The second thing that can be concluded from this brief study of industrial espionage is that there are a variety of methods by which espionage can take place. An employee revealing confidential information is perhaps the most common. However, compromising information systems is another increasingly popular means of obtaining confidential and potentially valuable data. You will want to know the best way to protect your company and yourself. In the upcoming exercises at the end of this chapter, you will run screen-capture software, key loggers, and antispyware.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. What is the ultimate goal of espionage?
   - **A.** To subvert a rival government
   - **B.** To obtain information that has value
   - **C.** To subvert a rival business
   - **D.** To obtain information not otherwise available
2. What is the best outcome for a spy attempting an espionage activity?
   - **A.** To obtain information without the target even realizing he did so
   - **B.** To obtain information with or without the target realizing he did so
   - **C.** To obtain information and discredit the target
   - **D.** To obtain information and cause harm to the target
3. What is the usual motivating factor for corporate/industrial espionage?
   - **A.** Ideological
   - **B.** Political
   - **C.** Economic
   - **D.** Revenge

4. Which of the following types of information would be a likely target for industrial espionage?
   - **A.** A new algorithm that the company's IT department has generated
   - **B.** A new marketing plan that the company has formulated
   - **C.** A list of all the company's customers
   - **D.** All of the above

5. Which of the following is a likely reason that an organization might be reluctant to admit it has been a victim of corporate espionage?
   - **A.** It would embarrass the IT department.
   - **B.** It would embarrass the CEO.
   - **C.** It might cause stock value to decline.
   - **D.** It might lead to involvement in a criminal prosecution.

6. What is the difference between *corporate* and *industrial* espionage?
   - **A.** None; they are interchangeable terms.
   - **B.** Industrial espionage only refers to heavy industry, such as factories.
   - **C.** Corporate espionage only refers to executive activities.
   - **D.** Corporate espionage only refers to publicly traded companies.

7. You can calculate the value of information by what formula?
   - **A.** Resources needed to produce the information, plus resources gained from the information
   - **B.** Resources needed to produce the information, multiplied by resources gained from the information
   - **C.** Time taken to derive the information, plus money needed to derive the information
   - **D.** Time taken to derive the information, multiplied by money needed to derive the information

8. If a company purchases a high-end UNIX server to use for its research and development department, what is probably the most valuable part of the system?
   - **A.** The high-end UNIX server
   - **B.** The information on the server
   - **C.** The devices used to protect the server
   - **D.** The room to store the server

9. Information is an asset to your company if it

   A. Cost any sum of money to produce
   B. Cost a significant sum of money to produce
   C. Might have economic value
   D. Might cost significant money to reproduce

10. What is the greatest security risk to any company?

   A. Disgruntled employees
   B. Hackers
   C. Industrial spies
   D. Faulty network security

11. Which of the following is the best definition for *spyware*?

   A. Software that assists in corporate espionage
   B. Software that monitors activity on a computer
   C. Software that logs computer keystrokes
   D. Software that steals data

12. What is the highest level of security you can expect to obtain?

   A. A level of security that makes the effort required to get information more than the value of the information
   B. A level of security comparable with government security agencies, such as the Central Intelligence Agency
   C. A level of security that has a 92.5% success rate in stopping intrusion
   D. A level of security that has a 98.5% success rate in stopping intrusion

13. In the context of preventing industrial espionage, why might you wish to limit the number of company CD burners and control access to them in your organization?

   A. An employee could use such media to take sensitive data out.
   B. An employee could use such media to copy software from the company.
   C. CDs could be a vehicle for spyware to get on your system.
   D. CDs could be a vehicle for a virus to get on your system.

14. Why would you want to scan an employee's computer when he leaves the organization?
    A. To check the work flow prior to leaving
    B. To check for signs of corporate espionage
    C. To check for illegal software
    D. To check for pornography
15. What is the reason for encrypting hard drives on laptop computers?
    A. To prevent a hacker from reading that data while you are online
    B. To ensure that data transmissions are secure
    C. To ensure that another user on that machine will not see sensitive data
    D. To prevent a thief from getting data off of a stolen laptop

EXERCISES

EXERCISE 7.1: Learning About Industrial Espionage

1. Using the Web, library, journals, or other resources, look up a case of industrial or corporate espionage not already mentioned in this chapter.
2. Write a brief essay describing the facts in the case. The parties in the case and the criminal proceeding are of interest, but most of your discussion should focus on the technical aspects of the case. Be sure to explain how the espionage was conducted.

EXERCISE 7.2: Using Antispyware

Note that this exercise may be repeated with different antispyware products. It is a good idea for any person interested in computer security to be familiar with multiple antispyware products.

1. Go to the website of one of the antispyware utilities. (See Chapter 5 if you need more direction.)
2. Find instructions on the vendor's website.
3. Download the trial version of that software.
4. Install the software on your machine.
5. After installation, run the utility. What did it find? Record your results.
6. Let the utility remove or quarantine anything it found.

EXERCISE 7.3: Learning About Key Loggers

Note that this exercise may only be completed on machines where you have explicit permission to do so (no public computers).

1. Using any website, find and download a key logger. The following websites might help you locate a key logger:

   www.kmint21.com/familykeylogger/
   www.blazingtools.com/bpk.html

2. Install the key logger on your PC.
3. Examine how the key logger behaves on your machine. Do you notice anything that might indicate the presence of illicit software?
4. Run the antispyware software you downloaded in Exercise 2. Does the antispyware software detect the key logger?

EXERCISE 7.4: Screen-Capture Spyware

1. Using the Web, find and download a screen-capturing spyware application. The following website might be helpful to you in selecting an appropriate product. Warning: Since you are downloading spyware, it is likely that your system's antivirus/antispyware will give you a warning on some of these sites:

   http://en.softonic.com/s/screen-capture-spy-software

2. Install and configure the application on your computer.
3. Run the application and note what it finds.
4. Run the antispyware from Exercise 2 and see whether it detects your spyware program.

EXERCISE 7.5: Learning About Hardware-Based Key Loggers

In this chapter, as well as in Chapter 5, we discussed software-based key loggers. However, there are also hardware-based key loggers.

1. Use the Internet to learn more about hardware-based key loggers. (You may wish to search for "Keykatcher" as a starting point.)
2. Write an essay outlining the way in which these key loggers work and how they could be implemented for either security or industrial espionage.

PROJECTS

PROJECT 7.1: Preventing Corporate Espionage

Using one of the websites listed in this book (you can also choose from the preferred resources in Chapter 1) or other resources, find a set of guidelines on general computer security. Write a brief essay comparing and contrasting those guidelines against the ones given in this chapter. Keep in mind that the guidelines in this chapter relate specifically to corporate espionage and not to general computer security.

PROJECT 7.2: Handling Employees

Write a brief essay describing steps regarding the handling of employees. Include all steps that you believe an organization should take to prevent corporate espionage. It is important that you support your opinions with sources and reasons.

If possible, visit a company and talk with someone in either the IT or personnel departments to determine how that company handles issues such as employee termination, rotation of duties, control of access to data, and so forth. Compare and contrast your steps to those used by the company you visited.

PROJECT 7.3: Asset Identification in Your Organization

Using the Asset Identification table found in this chapter or a similar table of your own design, identify the most valuable data in your organization (school or business) and what parties would most likely wish to access that data. Then write a brief guideline on how you might go about securing that data. In this project, you should tailor your security recommendations to the specific type of data you are trying to protect and against the most likely perpetrators of industrial espionage.

Case Study

David Doe is a network administrator for the ABC Company. David is passed over for promotion three times. He is quite vocal in his dissatisfaction with this situation. In fact, he begins to express negative opinions about the organization in general. Eventually, David quits and begins his own consulting business. Six months after David's departure, it is discovered that a good deal of the ABC Company's research has suddenly been duplicated by a competitor. Executives at ABC suspect that David Doe has done some consulting work for this competitor and may have passed on sensitive data. However, in the interim since David left, his computer has been formatted and reassigned to another person. ABC has no evidence that David Doe did anything wrong.

What steps might have been taken to detect David's alleged industrial espionage? What steps might have been taken to prevent his perpetrating such an offense?

This page intentionally left blank

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q-R

S

T

U

V

W

X-Y

Z