The Problem

The huge data theft at discount retail conglomerate TJX Companies illustrated the hackers’ trend toward profit-motivated cybercrimes. Hackers sought to rob TJX of its most valuable information. TJX operates about 2,500 retail locations in North America and Europe, including T.J. Maxx, Marshalls, HomeGoods, and AJWright. The company reported that a network intrusion had compromised some of its customers’ personal data—credit and debit card and driver’s license data.

TJX officials said that outsiders gained access to the computer network that stored customers’ credit card, debit card, and check information. The information involved was drawn from stores in the United States, Puerto Rico, Canada, the United Kingdom, and Ireland. A majority of the data related to individuals who shopped at its stores between 2003 and 2008.

The massive data breach seemed to involve someone who had TJX’s encryption key. But it might not have been needed since the cyberthief was accessing data during the card-application process before it was encrypted. The intruders had planted software in TJX’s systems to capture data throughout the day and then did a “postevent cleanup” to eliminate traces of the software. In effect, TJX’s network was infected by a computer worm that was placed on its mission-critical systems. That worm remained there undiscovered for 18 months.

The Response

In response to this incident, TJX did the following:

- Worked with all major credit and debit card firms to help investigate potential fraud.
- Worked with law enforcement officials including the U.S. Department of Justice, U.S. Secret Service, and the Royal Canadian Mounted Police.
- Directly contacted customers whose information was known to have been exposed because of the intrusion.
- Offered additional customer support to people concerned that their data may have been compromised.
- TJX spent $5 million in a three-month period dealing with this breach including costs incurred to investigate and contain the network intrusion, harden computer security and systems, communicate with customers, and technical, legal, and related fees.

In addition, several banks issued warnings to customers whose data may have been involved in the incident, as have the credit card brokers.

Containment via a Quiet Period

TJX delayed revealing details of the intrusion at the request of law enforcement officials. This quiet period has become a common practice to give investigators time to gather evidence of data incidents before making details of the events known to the public.

Hardening Information Security

TJX significantly strengthened its computer and network security after the incident and hired IT specialists General Dynamics and IBM to help investigate and assess how much data had been stolen.

Ben Cammarata, chairman of TJX Companies, issued a statement to reassure its customers as well as investors. He stated:

Since discovering this crime, we have been working diligently to further protect our customers and strengthen the security of our computer systems, and we believe customers should feel safe shopping in our stores. Our first concern is the potential impact of this crime on our customers, and we strongly recommend that they carefully review their credit card and debit card statements and other account information for unauthorized use.

Lessons Learned

This network intrusion highlights the unending efforts of criminals (hackers and malware code writers) to target massive databases of consumer information. That information is then sold to other parties for basic fraud, identity fraud, and other crimes. Dr. David Taylor, vice president of data security strategies at security software maker Protegrity Corporation in Stamford, Connecticut, warned that information stolen directly from computer databases will be used in criminal activity more often and more quickly, than data residing on misplaced equipment.

While a majority of the high-profile data incidents reported over the last several years have involved lost or stolen laptop computers, or misplaced backup storage tapes, there have also been a string of incidents that reflect criminal attempts to steal valuable corporate information.

There are thousands of security breaches every hour. Here we have compiled a few illustrative examples. In January 2007, TJX Companies disclosed that data from 100 million credit and debit cards had been stolen by hackers starting in July 2005. TJX’s data heist was the largest breach ever to date based on the number of records involved.

Following the disclosure, banks said that tens of millions of dollars of fraudulent charges were made on the cards. The Massachusetts Bankers Association sued TJX for negligence. The FTC filed a complaint alleging TJX did not have the proper security measures in place to prevent unauthorized access to the sensitive, personal customer information. The total cost of the data breach was an estimated $197 million. To compare this cost to TJX’s financials, see google.com/finance?fstype=ia&q=NYSE:TJX.

Questions

1. How did intruders gain access to TJX’s customer data?
2. For how long did the intrusion go undetected? Why?
3. What costs did TJX incur as a result of this intrusion?
1. Increasingly sophisticated website attacks that exploit browser vulnerabilities—especially on trusted websites. Website attacks on browsers are targeting components, such as Flash and QuickTime, which are not automatically patched when the browser is patched. Also, website attacks are more sophisticated attacks that can disguise their destructive payloads (the malicious part of the malware). Attackers are putting exploit code on popular, trusted websites that visitors believe are secure. Putting hidden attack tools on trusted sites gives attackers a huge advantage.

2. Increasing sophistication and effectiveness in botnets. Storm worm, which was not a worm, began spreading in January 2007 with an e-mail saying, “230 dead as storm batters Europe,” and was followed by subsequent variants. Within a week, it accounted for one out of every 12 infections on the Internet, installing rootkits (sets of network administration tools to take control of the network) and making each infected system a member of a new type of botnet. Previous botnets used centralized command and control; the Storm worm used peer-to-peer (P2P) networks to launch (control) the attack, so there is no central controller to take down to stop it. New variants and increasing sophistication will keep Storm worm and other even more sophisticated worms as serious threats.

3. Cyber espionage efforts by well-resourced organizations looking to extract large amounts of data and phishing. One of the biggest security stories of 2009 was the disclosure the theft of terabytes of data from federal agencies and defense contractors. Economic espionage will increase as nations steal data to gain economic advantage in multinational deals. The attack involves targeted phishing with attachments, using social engineering methods so the victim trusts the attachment.

4. Mobile phone threats, especially against the iPhone and VoIP. Mobile phones are general purpose computers so they are targeted by malware. A mobile platform is also a platform for unforeseen security risks. The developer toolkits provide easy access for hackers. Vulnerabilities of VoIP phones and attack tools that exploit those vulnerabilities have been published on the Internet.

5. Insider attacks. Insiders have a significant head start in attacks that they can launch. Insider-related risk as well as outsider-related risk has skyrocketed. Organizations need to put into place substantial defenses against this kind of risk, one of the most basic of which is limiting access according to what users need to do their jobs. This includes data leaks (such as in the WikiLeaks case).

6. Advanced identity theft from persistent bots. A new generation of identity theft is being powered by bots that stay on machines for 3 to 5 months collecting passwords, bank account information, surfing history, frequently used e-mail addresses, and more. They will gather enough data for advanced identity theft until criminals have enough data to pass basic security checks.

7. Increasingly malicious spyware. Criminals and nations continue to improve the capabilities of their malware. Additionally, some of the Storm variants are able to detect investigators’ activity and respond with a DoS attack against the investigators, making investigation more difficult. Advanced tools will resist antivirus, antispyware, and antirootkit tools to help preserve the attacker’s control of a victim machine. In short, malware will become stickier on target machines and more difficult to shut down.

8. Web application security exploits. Large percentages of websites have vulnerabilities resulting from programming errors. Adding to the risk exposure are Web 2.0 applications that are vulnerable because user-supplied data (which could have been supplied by hackers or others with malicious intent) cannot be trusted. By 2011 CWE/SANS cataloged the Top 25 Most Dangerous Software Errors. This is a list of the most widespread and critical errors that can lead to serious vulnerabilities in software that are often easy to find and abuse. The Top 25 list is a tool for education and awareness to help programmers to prevent the kinds of vulnerabilities; software customers can use the list to help (continued)
Examples of Internet Fraud

1. **Oprah’s Millionaire Contest Show** The scam sent an e-mail claiming that the recipient had been nominated to be on an *Oprah* show during which the cash winner would be named. Those “chosen” for the show are told to send money to pay for an airline or train ticket to Chicago for the program. They even have to pay to get into the show. (The show is free!) For additional Oprah scams, see: oprah.com/article/oprahdotcom/scams.

2. **Typical Phrases in E-Mail Fraud** These were compiled from microsoft.com/protect/fraud/phishing/prevent.aspx.

   - “Verify your account.” Businesses do not ask you to send passwords, log-in names, social security numbers, or other personal information through e-mail. If you receive an e-mail asking for this information, it is a scam.

   If you receive an e-mail message from Microsoft asking you to update your credit card information, do not respond: this is a phishing scam. To learn more, read fraudulent e-mail that requests credit card information sent to Microsoft customers at microsoft.com/uk/protect/yourself/phishing/msphishing.mspx.

(continued)
“You have won the lottery.” The lottery scam is a common phishing scam known as advanced fee fraud. One of the most common forms of advanced fee fraud is a message that claims that you have won a large sum of money, or that a person will pay you a large sum of money for little or no work on your part. The lottery scam often includes references to well-known companies.

“If you don’t respond within 48 hours, your account will be closed.” These messages convey a sense of urgency so that you’ll respond immediately without thinking. A phishing e-mail message might even claim that your response is required because your account might have been compromised.

3. Spoofed Websites Fake, copycat websites are also called spoofed websites. They are designed to look like the legitimate site, sometimes using graphics or fonts from the legitimate site. They might even have a Web address that’s very similar to the legitimate site you are used to visiting (e.g., verify-microsoft.com).

Once you are done at one of these spoofed sites, you might unwittingly send personal information to the con artist. If you enter your log-in name, password, or other sensitive information, a criminal could use it to steal your identity.

Next we show an example of the kind of phrase you might see in an e-mail message that directs you to a spoofed phishing site.

“Click the link below to gain access to your account.” Phishing links that you are urged to click in e-mail messages, on websites, or even in instant messages may contain all or part of a real company’s name and are usually masked, meaning that the link you see does not take you to that address but somewhere different, usually an illegitimate website.

Example of a masked Web address:
http://www.woodgrovebank.com/loginscript/user2.jsp

Notice in this example that resting (but not clicking) the mouse pointer on the link reveals the real Web address, which is shown under the masked URL.

4. Spring Break Offers Scammers (and or spammers) offer free or extremely inexpensive “deals,” such as:

- Experience Cancun with a complimentary accommodation.
- Four days and three nights in beautiful Cancun, Mexico, for free.
- Need a vacation? Get great travel deals sent right to your inbox.

While the promise of a “free” vacation may be appealing, it is important to remember a few facts about these offers. The offer came from a spammer who may use your personal information such as credit card details you provided for their own ulterior motives. Some spam messages provide “a disclaimer” stating that the traveler would be responsible for all applicable incidental hotel taxes and transportation costs. Consumers should be reminded that “there is no such thing as a free lunch” or a free vacation.

5. Getting “Paid” to Write Blogs The e-mail message indicates that “Freelance Writers are needed” to “Post in Blogs” in order to get paid $12 to $50 per hour. Just write one or two short, simple articles or blog posts everyday and you’ll be bringing in several hundred dollars of cold hard cash per week, almost effortlessly! Sounds good right? But then the catch . . . As soon as you log in to our exclusive, members-only area . . . For only $2.95, you will be asked to provide personal contact information and credit card details. The sites may lure recipients into a false sense of security by putting two security logos to tout the supposed reliability of dealing with this site.

6. Too Good to Believe All the Way from West Africa This was received by one of the book’s authors.

FROM: DESK OF DR. XYZ
AUDITING AND ACCOUNTING SECTION OF BANK OF AFRICA (B.O.A.)
OUAGADOUGOU BURKINA-FASO

Dear Friend:

I know that this mail will come to you as a surprise. I am the director in charge of auditing and accounting section of Bank of Africa Ouagadougou Burkina Faso in West Africa. I hoped that you will not expose or betray this trust and confident that I am about to expose you for the mutual benefit of our both families.

We need your urgent assistance in transferring the sum of $10.5 million United States dollars immediately to your account. The money has been dormant for years in our Bank here without anybody coming for it. We want to release the money to you as the nearest person to our deceased customer (the owner of the account) who died along with his supposed next of kin in an air crash in July 2000.
We don’t want the money to go into our bank treasury as an abandoned fund. So this is the reason why I contacted you, so that we can release the money to you as the nearest person to the deceased customer. Please we would like you to keep this proposal as a top secret and delete if you are not interested. Upon receipt of your reply, I will send you full details on how the business will be executed and also note that you will have 35% of the above mentioned sum if you agree to transact the business with us.

In acceptance the following information stated below you are required to provide us with:

1. Your age
2. Your full name and address
3. Your marital status
4. Your occupation/profession
5. Your direct telephone/fax numbers
6. Your passport details for legal operations
7. Your bank account details

Yours Sincerely,
Dr. XYZ

P.S.: Make sure you keep your transaction as your top secret and make it confidential till we receive the fund into the account that you will provide to the bank. Don’t disclose it to anybody “Please,” because the secrecy of this transaction is as well as the success of it.

7. Making a Fortune from Political Misery
Here is another e-mail received by one author:
Dear Friend,

I am Marina Litvinenko, wife of Alexander Litvinenko, a former Russian security officer who died in London hospital after apparently being poisoned with the highly-toxic metal thallium by Mr. Lugovoi, a Russian Government Paid agent.

This is my husband’s life in a video for your full understanding . . . Please I want you to assist me to remove US$9.5M given to my husband before his death by Mr. Berezovsky, a Russian Billionaire exiled in UK for exposing an alleged plot to assassinate him by the Russian Authority and to investigate the death of Anna Politkovskaya, a Russian Journalist believed to have equally been poisoned by the Kremlin for writing a book: The Putin’s Russia: Life in a Falling Democracy depicted Russia as a country where human rights are routinely trampled.

The funds are deposited with a financial firm in Europe and I will want to relocate these funds for investment in your region and with your assistance and advice.

As soon as I receive the response, I will furnish you with more details on this issue that is stressing me so badly. I do not mind drawing a business agreement with you.

Best regards,
Mrs. Marina Litvinenko

8. An Example of a Spoof E-Mail

From: The National Credit Union Administration (comes with an impressive logo)

Dear Credit Union Member:

You have received this e-mail because you or someone had used your account from different locations. For security purpose, we are required to open an investigation into this matter.

In order to safeguard your account, we require that you confirm your online banking details.

The help speed up to this process, please access the following link so we can complete the verification of your Credit Union Online Banking Account registration information.

http://www.ncua.gov/administration/auth/Authorize?=Submit

(continued)
Online File W9.3 (continued)

If we do not receive the appropriate account verification within 48 hours, then we will assume this Credit Union account is fraudulent and will be suspended.

The purpose of this verification is to ensure that your bank account has not been fraudulently used and to combat the fraud from our community.

We appreciate your support and understanding and thank you for your prompt attention to this matter.

Thank you,
Credit Union Security Department

This was sent to one of your authors who does not even have a credit union account.

9. With 1.3 Billion Chinese, You Can Get Rich Quickly In early March 2009, a Chinese scammer sent millions of e-mails in China, requesting borrowers to return to him, Mr. Wang (a very common name in China), the money he lent them, or...Within a week, hundreds of people who owed money to any Mr. Wang sent money to the mailbox provided in the e-mail (for a total of $200,000). The police were alerted, and the criminal was apprehended.

10. Phishing That Plays on Economic Fears Today’s economic turmoil delivers unprecedented opportunities for criminals to exploit victims. For instance, popular scams include phishing e-mails that look like they are coming from a financial institution that recently acquired the target victim’s bank, savings and loan, or mortgage holder. The large amount of merger and acquisition activity taking place creates an atmosphere of confusion for consumers, exacerbated by the dearth of consistent communications with the customer. Phishers thrive in this type of situation.

11. Blended Phishing/Malware Threats To increase success rates, some attacks combine phishing with malware for a blended attack model. For instance, a potential victim receives a phishing e-card via e-mail that appears to be legitimate. By clicking on the link inside the e-mail to receive the card, the person is taken to a spoofed website that downloads a Trojan to the victim’s computer. Alternatively, the victim may see a message that indicates a download of updated software is needed before the victim can view the card. When the victim downloads the software, it is actually a keylogger.

12. Texting and Mobile Phone Phishing Scams Posing as a real financial institution, phishers are using SMS as an alternative to e-mail to attempt to gain access to confidential account information. Known as “smishing,” the typical scam informs the mobile phone user that the person’s bank account has been compromised or credit card/ATM card has been deactivated. The potential victim is directed to call a number or go to a spoofed website to reactivate the card. Once on the site, through an automated phone system, the potential victim is then asked for card and account numbers and PIN numbers.

Online File W9.4 What Firewalls Can Protect

- **Remote log-in.** When someone connects from the outside to your PC and gains control of it. Examples: being able to view or access your files; running programs on your PC.
- **Application backdoors.** Some programs have special features that allow for remote access. Others contain bugs that provide a back door, or hidden access, which provides some level of control of the program.
- **Spam.** Spam is the electronic equivalent of junk mail. Spam can be dangerous. Often it contains links to dangerous websites.
- **SMTP session hijacking.** SMTP is the most common method of sending e-mail over the Internet. By gaining access to a list of e-mail addresses, a person can send spam to thousands of users. This is done quite often by redirecting the e-mail through the SMTP server of an unsuspecting host, making the actual sender of the spam difficult to trace.
- **Macros.** To simplify complicated procedures, many applications allow you to create a script of commands that the application can run. This script is known as a macro. Hackers create their own macros that, depending on the application, can destroy your data or crash your PC.
- **Viruses.** Range from harmless messages to erasing all your data.

(continued)
### Packet Filtering

Some firewalls filter data and requests from the Internet to a private network based on the network IP addresses of the computer sending or receiving the request. These firewalls are called *packet-filtering routers*. Packet filters are rules that can accept or reject incoming packets based on source and destination addresses and the other identifying information. Some simple examples of packet filters include the following:

- **Block all packets sent from a given Internet address.** Companies sometimes use this to block requests from computers owned by competitors.
- **Block any packet coming from the outside that has the address of a computer on the inside.** Companies use this type of rule to block requests where an intruder is using his or her computer to impersonate a computer that belongs to the company.

However, packet filters have their disadvantages. In setting up the rules, an administrator might miss some important rules or incorrectly specify a rule, thus leaving a hole in the firewall. Additionally, because the content of a packet is irrelevant to a packet filter, once a packet is let through the firewall, the inside network is open to data-driven attacks. That is, the data may contain hidden instructions that cause the receiving computer to modify access control or security-related files.

Packet-filtering routers often are the first layer of network defense. Other firewalls form the second layer.

### ONLINE FILE W9.5

#### Application Case

**HONEYNETS AND THE LAW**

Millions of networks and computers are on the Internet. Given this, what is the chance that an outside intruder will victimize a small collection of computers connected to the Internet? In the first phase of the Honeynet Project, which ran from 1999 to 2001, the honeynet consisted of eight honeypots that mimicked a typical home computer setup. Within 15 minutes of being connected to the Internet, one of the honeypots was hit. Over the course of the next few days, all the honeypots were compromised, and over the course of the next two years, they were attacked repeatedly.

During the first phase, many of the attacks were crude and fairly innocuous. Today, the character of both the intrusions and the intruders has changed. The proportion of hackers involved in illegal activities of all sorts has risen dramatically. If a company deploys a honeynet, there is a good chance that it will be the scene of a cybercrime or contain evidence of a crime. Some intruders may be focused solely on attacking the honeynet itself. Others may want to use it as a zombie for launching attacks, as a place to store stolen credit cards, or as a server to distribute pirated software or child pornography. Regardless, companies need to understand the types of crimes that may occur and the legal issues that may ensue if they choose to either report or ignore these crimes. Just because the activities on a honeynet are perpetrated by intruders, it does not mean that the operator has unlimited rights to monitor the users of the network.

Although many crimes can be perpetrated against or with a honeynet, the most frequent and obvious crime is network intrusion. The Computer Fraud and Abuse Act (CFAA) is a federal law passed by the U.S. Congress in 1986 intended to reduce “hacking” of computer systems. It was amended in 1994, 1996, and 2001 by the USA PATRIOT Act. The CFAA makes it a crime to attack “protected computers,” including computers “used in interstate or foreign commerce or communication.” If a computer is on the Internet, it is used in interstate communication. The CFAA protects all government computers and those used by banks and financial institutions. This means that the CFAA is going to protect most honeynets.

The act also defines the types of attacks that constitute a crime. It is a felony if an attacker “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.” Damage occurs when there is “any impairment to the integrity or availability of data, a program, a system or information.” The limitations are that in order for an attack to be a felony, one or more of the following must result: aggregate damage of at least $5,000; modification or impairment to the medical examination, diagnosis, treatment, or care of one or more individuals; physical injury to a person; a threat to public health or safety; or damage to a government computer used (continued)
for the administration of justice, national defense, or national security. Under these provisions, the act covers a wide range of activities, including:

- DoS attacks, viruses, and worms
- Simple intrusions in which the attacker causes damage
- Unauthorized information gathering, especially if the information is used for commercial advantage, financial gain, in furtherance of another crime, or the information is worth more than $5,000
- Unauthorized access to nonpublic U.S. government computers
- Using computers to obtain classified information without authorization
- Computer-related espionage, which may also constitute terrorism
- Trafficking in passwords
- Threatening to damage a computer
- Attempting to commit a network crime, even though the crime was never consummated

In running a honeynet, a company needs to be careful to ensure that it is not facilitating or helping further a crime. Precautions and actions must be taken to prevent potential or actual criminal activity from harming others; to inform authorities when criminal activities or evidence comes to light; and to ensure that the data, code, programs, and systems running on the honeynet are legal (e.g., do not store contraband on the system in an effort to trap an intruder).

The primary purpose of a commercial honeynet is to monitor and analyze intrusion and attacks. Under certain circumstances, the monitoring of these activities may constitute a criminal or civil action. In the United States, the federal Wiretap Act and the Pen Register, Trap, and Trace Devices statute place legal limits on monitoring activity.

The Wiretap Act makes it illegal to intercept the contents of a communication. If intruders cannot store (either directly or indirectly) data or information on a honeynet, then the act does not apply. If they can, then there are exceptions to the rule. For instance, if the monitoring is done to prevent abuse or damage to the system, then monitoring it is not illegal. The implication is that certain honeynet purposes and configurations are illegal and others are not.

In contrast to the Wiretap Act, the federal Pen Register, Trap, and Trace Devices statute applies to the “noncontent” aspects of a communication. For example, with telephones, telephone numbers are “noncontent.” Similarly, in a network communication, network addresses are “noncontent.” This statute makes it illegal to capture the noncontent information of a communication unless certain exceptions apply. The exceptions pertain primarily to actions that are taken by the communication provider (in this case the honeynet operator) to protect its rights or property. Again, certain honeynet purposes and configurations are legal and others are not.

When a company monitors the network activities of insiders and outsiders, a number of legal issues arise. Because monitoring is one of the primary activities of a honeynet, a company should consult legal counsel before deploying a honeynet and should become familiar with local law enforcement agencies that should be involved if illegal activities are observed.

Questions

1. What constitutes a crime under the CFAA?
2. What types of activities are prohibited by the CFAA?
3. What types of activities are illegal under the federal Wiretap Act? The Pen Register, Trap, and Trace Devices statute?

REFERENCES FOR ONLINE FILE W9.5


应用案例

如何公司对抗垃圾邮件

以下是一些成功对抗垃圾邮件的公司案例。

皮尔1进口

皮尔1连锁店的员工每天都要花很多时间来清理大量的垃圾邮件，整个电子邮件系统变得越来越麻烦而不是有帮助，当垃圾邮件占所有邮件的80%时。起初，皮尔1使用关键词过滤器来阻止公司认为不合适的邮件。这个系统失败了；IT部门阻止了合法的邮件，这些邮件具有双关意义。此外，垃圾邮件变得更加创新，使用了创造性拼写错误来避开过滤器。

皮尔1找到了一个合适的解决方案，MailFrontier Enterprise Gateway，它与Microsoft的电子邮件软件很好地配合。MailFrontier在Microsoft Exchange之前放置，以便检查所有传入的电子邮件。它接受良好的电子邮件并拒绝垃圾邮件。该软件使用17种预测技术，阻止98%的垃圾邮件。

Charter Communications

Charter Communications是第四大美国有线电视和互联网电缆公司，为2300万用户提供电子邮件账户，每天处理2亿封邮件。公司遭受滥用Charter的网络基础设施的垃圾邮件的困扰。垃圾邮件占总收入的50%以上。它也给客户带来了麻烦。Charter需要最小化垃圾邮件，同时保持信誉，防止被搜索引擎降级。Charter使用了两个独创工具：IronPort的C60电子邮件安全设备用于分类发送者（例如，IP地址、域名、发送者信誉），并为每个发送者提供特定的阈值。

谷歌（google.com/top/computers/internet/email/spam/filtering）和雅虎！（help.yahoo.com/l/us/yahoo/search/spam_abuse.html）已经采取了积极措施。例如，它们实施了垃圾邮件网站报告系统，建立了检查和惩罚欺骗性排名提升的做法，以及禁止违反者完全使用其搜索索引的网站。

谷歌警告说，它正在扩大其打击不良行为的措施，以清除不道德的技巧和做法。随着滥用行为的增加或不可接受，将通过法律来阻止，尽管这些法律的有效性可能各不相同。

防垃圾博客

博客所有者也可以使用Captcha工具（Completely Automated Public Turing test to tell Computers and Humans Apart），它在评论页面上使用验证测试来阻止脚本自动发布。这些测试可能要求人输入随机字符序列，而自动系统（软件脚本）不能阅读。

另一种可能有效的预防措施是只允许在博客上被检查后才发布的评论。但由于垃圾邮件者似乎占了上风，有时唯一的解决办法就是用户关闭评论功能。更多信息，请访问CAUCE网站（cauce.org）。
or rejection of e-mail messages. The second tool, Reputation Filtering, complements the first one. It allows e-mail administrators to sort e-mail senders based on the importance of the mail they send. Poor-quality messages are rejected.

**The Catholic Diocese of Richmond**
Managers of the information system at the Catholic Diocese of Richmond, Virginia, needed to stop the flow of spam to about 200 employees at three locations. The organization now is using Power Tools from Nemx (Canada). The tool achieves quality spam blocking by using the combination of modules including Content Manager, Concept Manager, Spam Manager.

**First Banking Services of Florida**
First Banking Services’ 250 employees use desktops to provide core data processing services to banks in the southeastern United States. The company is connected with many business partners, and its e-mail messages have different characteristics; many have large attachments. Spam was becoming a major problem. After careful evaluation, the company selected a spam-fighting solution called Mail Warden Pro (from Waterford Technologies, Ireland).

Mail Warden Pro allows users to set rules that distinguish spam from nonspam in a very flexible manner. The software also provides generic rules that have been found to be excellent in stopping spam and protecting against attachments with viruses. The volume of spam has been reduced from 65 percent of all e-mails to less than 5 percent.

**Questions**
1. The four companies use different blockers, each with a proprietary method. Why do each of the companies use different products from different vendors?
2. Regular spam stoppers from e-mail providers (e.g., Microsoft Exchange) were insufficient. However, such spam stoppers are getting better with time. Research the issues involved. Do you think that in the future the need for blockers such as those described here will wane?
3. In all cases, the companies felt that the investment in spam-fighting software was justifiable, but no formal ROI was done. Is this a reasonable approach? Why or why not?
4. What is the logic of combining antispam, antivirus, and antifraud software?

Even with tools such as Captcha turned on, it is risky to simply allow comments to go unchecked. Blog owners may be held responsible for anything illegal or defamatory posted on their blogs.

---

**REFERENCES FOR ONLINE FILE W9.6**

ironport.com (accessed March 2011).


---

**Online File W9.7 Auditing Information Systems**

An **audit** is an important part of any control system. Auditing can be viewed as an additional layer of control or safeguard. It is considered as a deterrent to criminal actions, especially for insiders. Auditors attempt to answer questions such as these:

- Are there sufficient controls in the system?
- Which areas are not covered by controls?
- Which controls are not necessary?
- Are the controls implemented properly?
- Are the controls effective? That is, do they check the output of the system?
- Is there a clear separation of duties of employees?

**audit**
An important part of any control system. Auditing can be viewed as an additional layer of controls or safeguards. It is considered as a deterrent to criminal actions especially for insiders.
Chapter Nine: E-Commerce Security and Fraud Protection

ONLINE FILE W9.8

Application Case

IMPACTS OF CHOICEPOINT’S NEGLIGENCE IN INFORMATION SECURITY

ChoicePoint is a leading data broker with access to 19 billion public records and information on more than 220 million individuals. The company collects personal information, including names, Social Security numbers, birth dates, employment information, and credit histories, which it then sells to over 50,000 businesses and government agencies. They rely on ChoicePoint’s data for customer leads, background checks, or other verification purposes.

The Problem
On February 15, 2005, ChoicePoint reported that the personal and financial information of 145,000 individuals had been “compromised” putting them at risk of identity theft. The compromise was not due to hackers or malicious spyware.

ChoicePoint had sold the information to Olatunji Oluwatosin, a 41-year-old Nigerian national living in California, who had pretended to represent several legitimate businesses—a technique that is called pretexting. Oluwatosin’s credentials had not been verified, which enabled him to set up bogus business accounts that gave him access to databases containing personal financial data. For their negligence and violation of their privacy policy, ChoicePoint faced state and federal penalties.

At the state level, ChoicePoint was compelled to disclose what had happened. California’s privacy breach notification law, Senate Bill 1386 (SB 1386), which went into effect in July 2003, required ChoicePoint to inform residents that their personal information had been compromised. Within days, outraged attorneys general in 38 other states demanded that the company notify every affected U.S. citizen.

At the federal level, ChoicePoint was charged with multiple counts of negligence for failing to follow reasonable information security practices. Beginning in 2001, the company had been receiving subpoenas from law enforcement authorities alerting them to fraudulent activity. Despite these warnings, management did not tighten customer approval procedures to safeguard access to confidential data. The Federal Trade Commission (FTC) charged ChoicePoint with violating the:

◗ Fair Credit Reporting Act (FCRA) by furnishing credit reports to subscribers who did not have a permissible purpose to obtain them; and by not maintaining reasonable procedures to verify their subscribers’ identities and intended use of the information.

◗ FTC Act by making false and misleading statements about its privacy policies on its website.

Section 5 of the FTC Act prohibits unfair or deceptive practices, which gives the FTC authority to take action against companies whose lax security practices could expose the personal financial information of customers to theft or loss. For a full explanation of the Act, see ftc.gov/privacy/privacyinitiatives/promises.html.

On March 4, 2005, ChoicePoint filed a report with the SEC warning shareholders of an expected $20 million decline in income by December 31, 2005, and a $2 million increase in expenses from the incident. In addition, there would also be FTC fines. In January 2006, the FTC announced that ChoicePoint had agreed to pay a $10 million fine, the agency’s largest-ever civil (continued)
penalty, plus $5 million to compensate customers for losses stemming from the data breach. Legal expenses of $800,000 were incurred in the first quarter of 2006 alone related to the fraudulent data access. With the announcement of the impending $15 million settlement, ChoicePoint’s stock price plunged.

The Solution
As part of the settlement, the FTC mandated the solutions to ChoicePoint’s risk exposure. The company implemented new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, established and maintains a comprehensive information security program, and obtains audits by an independent third-party security professional every other year until 2026. To reassure stakeholders and legitimate customers, ChoicePoint hired a chief privacy officer (CPO).

The Results
ChoicePoint’s data breach brought businesses’ security policies to national attention. Together with high-profile frauds and malware, data breaches have triggered increased corporate governance and accountability.

Questions
1. Why do you think that ChoicePoint did not verify all potential customers thoroughly before allowing them to open accounts?
2. What legal charges and fines were imposed on ChoicePoint for its negligence and violation of privacy policy?
3. What did ChoicePoint do to reassure stakeholders and customers?

REFERENCES FOR ONLINE FILE W9.8

ftc.gov (accessed March 2011).