Keeping Taxpayer Data Secure

This document is designed to provide general information and is not a substitute for professional advice in specific situations. It is not intended to be, and should not be construed as, legal or accounting advice which should be provided only by professional advisers.

Contents

Introduction to the Course

The annual global cost of cybercrime is high and getting higher all the time. In fact, cyber criminals reap a windfall from their activities that is estimated to have been $450 billion in 2015 and is anticipated to climb to an annual $6 trillion average by 2021. Almost all of that cybercrime began with—and continues to start with—a social engineering concept known as "phishing."

Certain business organizations, among which are those referred to as "financial institutions," are charged by the FTC with taking particular steps to protect their customers' financial information. Included in the category of financial institutions are professional tax preparers. Professional tax preparers normally maintain a significant amount of taxpayer information in various files—electronic and paper—that would be a treasure trove for cyber criminals.

In this course, tax preparers are introduced to the problem of cybercrime and its costs, offered methods that can be expected to reduce the chances of becoming a cybercrime victim, and informed of proper steps to take if they do become victims of cybercrime. This course is a basic tax level course with no prerequisites, and qualifies for 3 CE credits in the Tax Law category. Accordingly, it will examine cybercrime and will discuss:

- The extent of the cybercrime problem;
- The potential costs to a tax preparer whose taxpayer data has been breached;
- The best practices a tax preparer may implement to avoid becoming a cybercrime victim; and
- What a tax preparer should do if its taxpayer data has been breached.

Learning Objectives

Upon completion of this course, you should be able to:

- Recognize the pervasiveness of cybercrime;
- Identify the potential costs of experiencing a data breach;
- Understand the best practices that may be implemented to protect a tax preparer from cybercrime; and
- List the responsibilities of a tax preparer who has experienced a taxpayer data breach.

Chapter 1 – Introduction to Cybercrime

Introduction

The overwhelming majority of cybercrime begins with a confidence scam that makes a request from a cybercriminal seem reasonable. However, once the request is granted and the computer user clicks on a link to the website, malicious software is installed on the victim's computer. That malicious software—known commonly as "malware"—may result in one or more of a wide range of uniformly bad outcomes.

This chapter will discuss the social engineering concept known as "phishing" and will look at various software intrusions that often result from falling prey to it including:

- Computer viruses;
- Denial-of-service attacks;
- Trojan horses;
- Ransomware; and
- Spyware.

Chapter Learning Objectives

When you have completed this chapter, you should be able to:

- Identify the source of the most frequent type of malicious access to a firm's taxpayer information;
- List the most common types of cyber attack;
- Describe how a denial-of-service attack operates to impede business operations; and
- Recognize the dangers of Trojan horses.

The Nature of Cybercrime

The term "cybercrime" refers to criminal activities carried out by means of a computer or the Internet. An estimated 90% - 95% of that cybercrime began with—and continues to start with—a relatively simple social engineering confidence scam referred to as "phishing." However, before looking at phishing and the steps a tax preparer may take to avoid it, let's examine some of the types of cyber attack and their effects on the victim.

Although the primary motivation behind a cyber attack is likely to be financial—the ability of the criminal to make money by attacking the victim's computer, in other words—it may also be motivated by a desire simply to harm the victim by making the attacked system inoperable and putting the computer user out of business.

There are many variations of cybercrime, some of which overlap; however, the principal types of cyber attack involve:

- Computer viruses;
- Denial-of-service (DOS) attacks; and
- Malware.

Computer Viruses

Computer viruses are software programs that, once on your computer, copy themselves by modifying other computer programs on the attacked computer and inserting their own code in them. As a result of the attack, a computer virus may accomplish one or more of the following. It may:

- Access your private information stored on the computer, such as –
    - Credit card and other account numbers,
    - Social Security numbers, and
    - Your email address file;
- Disclose your computer keystrokes to the cyber criminal in order to provide passwords and other confidential information to a third party;
- Corrupt the data on your computer's hard drive, making it unusable;

- Take over your computer's hard disk space and dramatically slow its ability to work; or
- Cause the computer to stop working entirely.

Denial-of-Service Attacks

A denial-of-service attack is a cybercrime designed to stop users—you, your employees or your potential customers—from accessing a host website connected to the Internet. The attacked "host" may be a resource website that your firm uses or, alternatively, it may be your *firm's* website that is attacked to keep your potential customers from accessing it.

This kind of cyber attack is normally accomplished by flooding the host victim's computer with incoming messages. The result on a victim's computer can be compared to the commuter traffic delay that occurs when a major highway narrows from six lanes to two during rush hour. The flood of incoming messages is designed solely to make access to the host computer difficult or impossible for anyone else, the victim, the victim's clients, etc.. The denial-of-service may be temporary or may continue for an indefinite period.

A variation of the denial-of-service attack is known as a distributed-denial-of-service. A distributed denial-of-service attack differs from a simpler denial-of-service attack in that the incoming computer traffic originates from multiple sources rather than from a single source. Since the flood of incoming traffic in a distributed denial-of-service attack originates from many sources, it is far more difficult to block than it would be if it came from a single source, and its adverse effect on the victim may be even greater.

Installing Malware

The term "malware" is simply a contraction of the words ***malicious software*** and is used to refer generally to various types of harmful or intrusive software secretly installed and intended to act against the interests of the computer user. Thus, it includes:

- Trojan horses;
- Ransomware;
- Spyware; and
- Other software installed with malicious intent.

Once the malware is installed on the host computer, it becomes activated and performs the tasks it has been programmed to perform. The task it performs may copy files and give the attacker covert access to the computer, a type of malware we will look at just below when we discuss **Trojan Horses**.

Trojan Horses

A Trojan horse takes its name from Greek mythology, specifically from Homer's *Iliad*, a tale in which the Greeks—at war with inhabitants of the city of Troy—roll an enormous hollow statue of a horse filled with Greek warriors up to the city's gates. The Greeks planned to have the warriors emerge from the statue and sack the city when the Trojans rolled the horse through the city gates.

In more recent times, "Trojan horse" has come to refer to any surreptitious means by which a third person attempts to trick an adversary into willingly inviting a foe into an otherwise protected setting, such as hiding a computer virus in an apparently-benign Trojan horse program. The scam used to place computer malware known as a Trojan horse on a victim's computer often starts with the social engineering known as phishing (see **Phishing** below) in an attempt to encourage a computer user to open a harmless appearing attachment to an email. When that occurs, the malicious computer code contained in it begins to accomplish the tasks for which it was programmed.

The tasks to be accomplished by the malware in the Trojan horse may involve any number of malicious acts, including:

- Contacting a cybercriminal and providing a secret method allowing the criminal to bypass the computer's normal authentication system and enter it to permit the criminal to –

    - Gain access to an email account's address list, obtain passwords, steal personal identity or banking information, etc. in order to withdraw funds from an online banking account, brokerage account, or other source of cash, or
    - Infect other devices connected to a computer network; or
- Taking control of and shutting down a targeted computer and then demanding cash or other payment from the individual or business to again have access to the computer and its files. (See **Ransomware** below.)

Ransomware

Ransomware is another type of malicious computer code that may be lurking within a Trojan horse. This type of malware locks or encrypts the digital files contained on a business' computer. Such an attack enables the cyber criminal to then demand a ransom to again give the business access to its files. Often, any ransom paid fails to gain access to the infected computer or its files. According to the FBI's 2016 Internet Crime Report,[1] the inability of a business to access its important data "…can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation."

Ransomware attacks normally begin by a victim opening an email message and clicking on an attachment to the email that seems legitimate, such as an invoice or electronic fax. However rather than being an invoice, fax or any other legitimate item, the attachment actually contains the malicious ransomware computer code. Alternatively, the email, rather than having an attachment, contains a harmless appearing URL (Uniform Resource Locator) link better known as a web address. But, when the computer user clicks on the link, it leads to a website that infects the computer with malware.

Spyware

Spyware is computer code that, once downloaded, gathers information about the computer user without the user's consent or knowledge and transmits it to a third party. Much spyware—but certainly not all—is relatively benign, consisting of:

- Advertising-supported software known as "adware;" and
- Tracking cookies.

Adware is designed to cause advertisements—often unexpected and unwanted—to pop up when the user is on the Internet. The advertising that pops up is the result of the adware's analysis of the Internet sites the user normally visits and the types of goods or services featured on them. A tracking cookie, the second type of benign spyware noted, is designed to record the user's Internet browsing activity and, similar to adware, to cause pop-up ads to appear on the user's monitor. Adware and tracking cookies are generally not unlawful and may have been agreed to by the user as part of a website's terms of use.

In contrast to spyware that may be benign, other spyware falls squarely into the malicious code category and includes malware that collects and sends back the user's personal information, such as:

- Internet surfing habits;
- User logins; and
- Bank or credit account information.

Clearly, this malicious code version of spyware exposes the computer user and business clients whose files are on the computer to identity and other types of theft.

Phishing

It is reasonable to ask how a tax preparer or anyone else with a modicum of savvy—or even just awareness—could be duped into allowing a computer virus, a Trojan horse or other malicious software to attack his or her computer since the majority of cyber attacks require that a computer user download malicious software. Why wouldn't people just refuse to download any email attachment he or she was unsure of? The answer appears to lie principally with cyber criminals schooled in the art of deception and its use in computer crime, in short, through something called "phishing."

[1] Report may be accessed at https://pdf.ic3.gov/2016_IC3Report.pdf.

Phishing is a form of social engineering, i.e. using deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. It often involves contacting an intended victim—frequently via email—falsely claiming to be from the victim's Internet service provider, online brokerage or other provider of services and requesting that he or she provide information that the intended victim believes is needed in order for the contact to perform some task that will be beneficial for the victim. And, the victim believes the contact is looking out for his or her best interest in bringing this to his or her attention. In fact, doing what the contact requests will enable the cyber criminal to steal money, taxpayer records or other information from the victim.

The intended victim might be asked to verify:

- Computer passwords;
- Bank or brokerage account login information;
- Credit card information; or
- Other sensitive information.

Microsoft offers the following example of a phishing email addressed to an intended victim who uses the very popular Facebook:

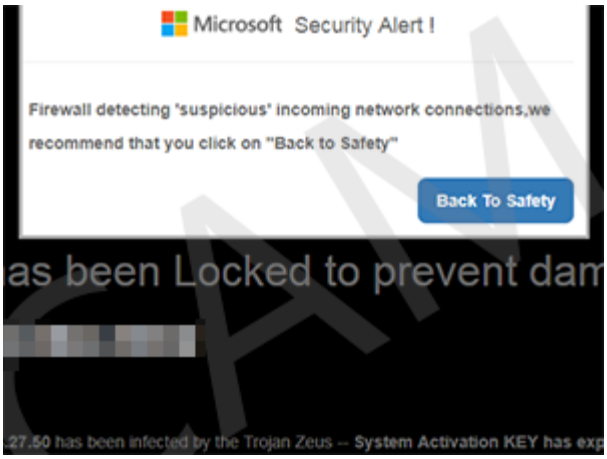
As Microsoft's website details, and as highlighted in the above example, phishing emails are often characterized by the following:

- Poor spelling and bad grammar;
- The presence of links in the email;
- The threat of an undesired loss if the addressee fails to take the requested action; and
- Identification of the sender with a legitimate and popular company—with Facebook in the example.

If an email contains a link to a website, it is a good idea NOT to click on it. However, if you just rest the cursor over the link, you can see the actual URL for the website to which clicking on the link will take you. (See the inset below taken from the Microsoft website.) If the address shown by hovering over the link fails to match the link typed into the message, you can be reasonably certain that it is a phishing attempt. However, even if the two addresses are identical, you still can't be sure the email is not a phishing attempt.

In order to encourage the intended victim of the phishing scam to act immediately, the cyber criminal may threaten the loss of some product, service or opportunity if the victim fails to act right away. Thus, the intended victim believes he or she has a clear choice: either accede to the request, complete the application (in the above example) and risk a *possible* cyber attack by this person who (the soon-to-be victim believes) is apparently acting in the individual's interest or permanently lose the desirable service.

A somewhat similar approach involves the statement that the computer's security has been compromised and that, in order to maintain the integrity of the data on the network, the intended victim should immediately contact the company at *1-800-LOOKOUT* or, as shown below, click on "Back to Safety."



Microsoft Security Alert!

Firewall detecting 'suspicious' incoming network connections, we recommend that you click on "Back to Safety"

It should be no surprise in light of the topic that once the recipient clicks on "Back to Safety" his status changes from ***intended victim*** to ***victim***.

A similar computer integrity scam might begin with the following notice being received on your email account:

Threats Detected Norton by Symantec Online Scan

Adware. DealPly has been detected. Contact Support

SYSTEM CRITICALLY INFECTED! CONTACT SUPPORT IMMEDIATELY. NORTON TECHNICAL SUPPORT

DO NOT TRY TO MANUALLY REMOVE THE VIRUS, HARD-DRIVE MIGHT FAIL*

The intended victim is warned against trying to remove the alleged virus (that isn't there yet) and directed to call "Toll Free Support" where the victim will be scammed.

In both these examples, the social engineer has likely gained some credibility in the mind of the intended victim by "spoofing," i.e. appearing to be associated with a popular website or company by employing graphics used by them: Microsoft in the first case and Norton in the second. Furthermore, the request made by the cyber criminal may appear entirely reasonable and appropriate in view of what has gone before. For example:

- The cybercriminal has "solved" your computer problems and just wants you to go to a website and install a free program that will keep the computer or network from having the problem again; or
- The cybercriminal will ask for your user name and password and request that you click on a URL to take you to a website that will enable the "helper" to access and fix your computer.

Once the requested information is passed to the cybercriminal, it usually doesn't take long for the damage to the victim's computer or computer network to begin. That damage may involve:

- Taking control of the computer and causing it to stop working until a ransom is paid;
- Copying files containing sensitive client taxpayer information, such as Social Security numbers, brokerage or bank account numbers; or
- Wreaking some other theft or damage.

The Internal Revenue Service regularly warns potential victims to beware of fake emails or websites looking to steal personal information, and it noted a recent significant increase in both phishing and malware incidents. In addition, the IRS has observed email schemes targeting tax professionals among others. In many of these schemes, criminals pose as a person or organization the targeted individual trusts or recognizes.

Frequent ruses used by these cybercriminals include:

- Hacking into an email account and sending mass emails under another person's name;
- Posing as a trusted institution, such as a –
    - Bank,
    - Credit card company,
    - Tax software provider, or
    - Government agency; and
- Creating legitimate-appearing websites that contain phony log-in pages in an attempt to obtain –
    - Passwords,
    - Social Security numbers, and
    - Other information that can lead to identity theft.

Criminals increasingly are targeting tax professionals, deploying various types of phishing emails in an attempt to access client data. To combat these cybercriminal attacks, the IRS, state tax agencies and the tax industry launched a public awareness campaign called *Protect Your Client; Protect Yourself* to warn tax professionals, offer tips and compile alerts. Tax professionals who receive unsolicited and suspicious emails that appear to be from the IRS or related to the e-Services program should report such incidents at *phishing@irs.gov*.

Summary

- 90% - 95% of cybercrime begins with a confidence scam referred to as "phishing," i.e. deception designed to manipulate individuals into divulging confidential or personal information, such as computer and other passwords, financial account login information, credit card numbers and other sensitive data that may be used for fraudulent purposes
- The principal types of cyber attack involve computer viruses, denial-of-service (DOS) attacks and Malware.
- Computer viruses may access various types of private information stored on the computer, disclose computer keystrokes to a third party, corrupt computer data, cause a computer to work more slowly or stop working entirely by taking over all available disk space.
- Denial-of-service attacks stop users from accessing a host computer connected to the Internet by overwhelming the attacked computer with traffic.
- "Malware" refers to various types of malicious software, such as Trojan horses, Ransomware, spyware and other software installed with malicious intent.
- A "Trojan horse" is a harmless-looking piece of software containing a computer virus or other malicious code that emerges when the apparently-harmless software has been accessed and may allow an attacker to bypass computer authentication and collect information to be used to withdraw money from an account, obtain personal financial information, infect other connected devices and/or hold a computer hostage.
- Ransomware, once downloaded, locks the user out or encrypts the digital files contained on a computer.
- Spyware is computer code that gathers information about a computer user without consent or knowledge for transmittal to a third party and may result in financial harm.

Chapter Review

1. Most cybercrime begins with:

A. installation of a computer virus

B. mail theft

C. phishing

D. a denial of service attack

2. A _____ is normally accomplished by flooding the host victim's computer with incoming messages in order to stop users from accessing the victim's website.

A. computer virus

B. denial-of-service attack

C. Trojan horse

D. tracking cookie

3. What can be done to determine if a URL link sent to you in an email is likely a phishing attempt?

A. Rest the cursor over the link to view the actual URL address

B. Call the telephone number contained in the email

C. Click on the link

D. Nothing can be done

Chapter 2 – Laws & Regulations Safeguarding Taxpayer Data

Introduction

Many federal, state, city and local government laws and regulations are in place to safeguard taxpayer data. This chapter will identify and briefly discuss the federal laws addressing privacy and security including the *Gramm-Leach-Bliley Act* and the *FTC Privacy of Consumer Financial Information Rule* and the *Safeguards Rule*.

Chapter Learning Objectives

When you have completed this chapter, you should be able to:

- List the principal federal laws and regulations governing the security of taxpayer information;
- Understand the objectives and requirements of the Safeguards Rule;
- Identify the notification requirements imposed by the Financial Privacy Rule; and
- Distinguish between a customer and a consumer under FTC regulations.

The Gramm-Leach-Bliley Financial Modernization Act

After the stock market crash of 1929, the senate committee on banking and currency began an investigation into its causes. And, in 1933, legislation providing federal insurance for bank depositors and requiring the separation of commercial and investment banking became the Banking Act of 1933, generally referred to as the Glass-Steagall Act.

Since its passage, banking industry interests have sought the removal of the barriers between the banking, securities and insurance industries erected by Glass-Steagall. In 1999, the Financial Services Modernization Act—better known as the Gramm-Leach-Bliley Act (GLB)—did just that. The GLB, among other things, directed the Federal Trade Commission (FTC) to establish the Financial Privacy Rule and the Safeguards Rule, both of which address tax preparers' vulnerability to cyberattacks. A brief discussion of each of those rules is provided below.

FTC Standards for Safeguarding Customer Information Rule

The Safeguards Rule requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

16 CFR § 314 codifies the Safeguards Rule and mandates that financial institutions—a category that includes ***professional tax preparers***, data processors, affiliates, and service providers—to meet three important objectives:

1. To insure the security and confidentiality of customer records and information[2];
2. To protect against any anticipated threats or hazards to the security or integrity of such records; and
3. To protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to the customer.

It also requires that financial institutions develop, implement and maintain a written and accessible Information Security Program. The Information Security Program must contain administrative, technical, and physical safeguards appropriate to the business' size and complexity, nature and scope of activities, and sensitivity of customer information it handles.

[2] The term "customer information" means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the firm or its affiliates.

Meeting FTC Safeguards Rule Requirements

To meet the requirements of the Safeguards Rule as outlined by the FTC, a financial institution is required to:

- Designate one or more employees to coordinate its information security program;
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- Design and implement a safeguards program, and regularly monitor and test it;
- Select service providers that can maintain appropriate safeguards, make sure the firm's contract requires them to maintain safeguards, and oversee their handling of customer information; and
- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The requirements are intentionally broad and designed to be flexible, allowing firms to implement safeguards appropriate to their own circumstances and the risks faced by their customers' data. For example, some companies may choose to put their safeguards program in a single document, while others may put their plans in several different documents—one to cover an information technology division and another to describe the training program for employees, for example. Similarly, a company may decide to designate a single employee to coordinate safeguards or may assign this responsibility to several employees who will work together.

In addition, companies must consider and address any unique risks raised by their business operations, such as the risks raised when employees access customer data from their homes or other off-site locations, or when customer data is transmitted electronically outside the company network.

FTC Privacy of Consumer Financial Information Rule

The Privacy of Consumer Financial Information Rule (otherwise known as the Financial Privacy Rule) aims to protect the privacy of their customers by requiring financial institutions, including professional tax preparers, data processors, affiliates, and service providers to give their customers privacy notices that explain the financial institution's information collection and sharing practices; in other words, the notices must identify:

- The types of information about customers the business collects; and
- To whom it makes the collected information available.

In turn, customers have the right to limit some sharing of their information by opting out. Also, financial institutions and other companies that receive personal financial information from a financial institution may be limited in their ability to use that information. The FTC Privacy Rule implements sections 501 and 502(b)(2) of the GLB requirements.

Requirements under the Privacy Rule

Pursuant to the privacy rule, financial institutions must give their customers—and, in some cases, their consumers—a "clear and conspicuous" written notice describing their privacy policies and practices. ***When*** the firm must provide the notice and ***what*** the firm must say depend on what the firm does with the information.

Individuals Who Must Receive a Privacy Notice

The firm's obligations with respect to sending a privacy notice depend on whether the firm's clients are "customers" or "consumers." In brief, the Privacy Rule requires the firm to give notice to all its customers about the firm's privacy practices. Additionally, if the firm shares consumer information in certain ways it must provide a privacy notice to its consumers as well.

Consumer Defined

The Privacy Rule defines a "consumer" as someone who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that person's legal representative. The term, however, does not apply to commercial clients, like sole proprietorships. Therefore, in cases in which the client is not an individual, or is an individual but is seeking the firm's product or service for a business purpose, the Privacy Rule does not apply.

Examples of consumer relationships include individuals:

- Cashing a check with a check-cashing company;
- Making a wire transfer; or
- Applying for a loan.

Customer Defined

A "customer" is defined as a consumer who has a continuing relationship with the firm. It is the nature of the relationship—whether or not it is an ***ongoing*** relationship—rather than its ***actual duration*** that defines the firm's customers. Even if an individual repeatedly uses the firm's services for unrelated transactions, she may not be considered a customer.

The FTC offers the following example: If an individual repeatedly uses the ATM at a bank where she does not have an account, those isolated transactions, no matter how frequent, do not make her that bank's customer. She would still be a consumer of that bank's services, however.

A former customer is one who has obtained a financial product or service from a financial institution but no longer has a continuing relationship with it. For purposes of the firm's obligations under the Privacy Rule, a former customer is considered to be a consumer rather than a customer.

An example of an individual having a customer relationship is one obtaining the services of a tax preparer or investment adviser.

Privacy Notices must be sent to Customers

Whether or not the firm shares customer non-public personal information (NPI), the firm must give all its customers a privacy notice. The firm is required to provide:

- An initial notice; and
- An annual notice.

The initial notice is normally expected to be provided by the time the customer relationship is established. However, if providing the initial notice no later than at the time of establishing the customer relationship would substantially delay the customer's transaction, the firm may provide the notice within a reasonable time after the customer relationship is established, ***but only if the customer agrees***. The annual notice must be provided to the customer for as long as the customer relationship lasts.

If the firm shares NPI with nonaffiliated third parties outside of the exceptions described below (see **Exceptions**), the firm also must give its customers:

- An "opt-out" notice explaining the individual's right to direct the firm not to share NPI with a nonaffiliated third party;
- A reasonable way to opt out; and
- A reasonable amount of time to opt out before the firm discloses the NPI.

Consumers Who Are Not Customers

Before the firm shares NPI with nonaffiliated third parties outside of the exceptions described below (see **Exceptions**), the firm must give its non-customer consumers a privacy notice, including an opt-out notice. If the firm doesn't share information with nonaffiliated third parties, or if the firm only shares such information within the exceptions, the firm does not have to give a privacy notice to its consumers.

If the firm is required under the FTC rules to provide a privacy notice to its consumers because of its NPI-sharing policies, the firm may choose to give them a short-form notice instead of a full privacy notice. The short-form notice must:

- Explain that the firm's full privacy notice is available on request;
- Describe a reasonable way consumers may get the full privacy notice; and
- Include an opt-out notice.

The Contents of the Privacy Notice

The firm's notice must accurately describe how the firm collects, discloses, and protects NPI about consumers and customers, including former customers. The notice must include, where applicable to the firm, the following information:

- Categories of information collected. For example, whether the nonpublic personal information is obtained from an application or a third party such as a consumer reporting agency.
- Categories of information disclosed. For example, the categories of information disclosed may be –
    - Information obtained from an application, such as the individual's name, address, and/or phone number;
    - The individual's Social Security number;
    - Account information; and/or
    - Account balances.
- Categories of affiliates and nonaffiliated third parties to whom the firm discloses the information. For example, is NPI disclosed to financial services providers, such as mortgage brokers and insurance companies; or to non-financial companies, such as magazine publishers, retailers, direct marketers, and nonprofit organizations. The firm also may describe categories of other nonaffiliated parties to whom it may disclose NPI in the future.
- Categories of information disclosed and to whom disclosed under the joint marketing/service provider exception in section 313.13 of the Privacy Rule (see **Exceptions**).
- If the firm is disclosing NPI to nonaffiliated third parties under the exceptions in sections 313.14 (exceptions for processing or administering a financial transaction) and 313.15 (exceptions, including fraud prevention or complying with federal or state law and others) of the Privacy Rule (see **Exceptions**), a statement that the disclosures are made as permitted by law.
- If the firm is disclosing NPI to nonaffiliated third parties, and that disclosure does not fall within any of the exceptions in sections 313.14 and 313.15, an explanation of consumers' and customers' right to opt out of these disclosures (see **Opt-Out Notices**).
- Any disclosures required by the Fair Credit Reporting Act.
- The firm's policies and practices with respect to protecting the confidentiality and security of NPI. (Click here to see FTC tips on **Safeguarding NPI**.)

The firm only needs to address those items listed above that apply to the firm. For example, if the firm doesn't share NPI with affiliates or nonaffiliated third parties except as permitted under sections 313.14 and 313.15, the firm can provide a simplified notice that: (1) describes the firm's collection of NPI; (2) states that the firm only discloses NPI to nonaffiliated third parties "as permitted by law;" and (3) explains how the firm protects the confidentiality and security of NPI.

The Appearance of the Privacy Notice

The privacy notice must be "clear and conspicuous," whether it is on paper or on a website. It must be reasonably understandable, and designed to call attention to the nature and significance of the information. The notice should use plain language, be easy to read, and be distinctive in appearance. A notice on a website should be placed on a page that consumers use often, or it should be hyperlinked directly from a page where transactions are conducted.

Safeguarding NPI

The FTC has issued a separate rule to address the requirements for safeguarding NPI. See 16 CFR Part 314, 67 Fed. Reg. 36484 (May 23, 2002). The firm should consult the FTC's website for more information about this rule and further guidance for small businesses in implementing the Safeguards Rule requirements.

The Privacy Rule requires that the firm's privacy notice provide an accurate description of its current policies and practices with respect to protecting the confidentiality and security of NPI. For example, if the firm restricts access to NPI to employees who need the information to provide products or services to the firm's consumers or customers, say so.

Delivering Privacy Notices

The firm must deliver its privacy notices to each consumer or customer in writing, or, if the consumer or customer agrees, electronically. The firm's written notices may be delivered by mail or by hand. For individuals who conduct transactions with the firm electronically, the firm may post its privacy notice on its website and require them to acknowledge receiving the notice as a necessary part of obtaining a particular product or service.

For annual notices, the firm may reasonably expect that its customers have received the firm's notice if they use its website to access the firm's financial products or services and agree to receive notices at its website, and the firm posts its notice continuously in a clear and conspicuous manner on its website.

Notices given orally or posted in the firm's office(s) don't comply with the rule.

Opt-Out Notices

If the firm shares NPI with nonaffiliated third parties outside of three exceptions (see **Exceptions**), it must give its consumers and customers an "opt-out notice" that clearly and conspicuously describes their right to opt out of the information being shared. An opt-out notice must be delivered with a privacy notice, and it can be part of the privacy notice.

The opt-out notice must describe a way for consumers and customers to opt out that is considered reasonable ***before*** the firm can disclose their NPI to these nonaffiliated third parties. Although requiring the consumer or customer to write a letter as the only way to opt out would not be deemed acceptable, reasonable means to opt out include:

- A toll-free telephone number; or
- A detachable form with a check-off box and mailing information.

While the GLB does not require the firm to provide an opt-out notice if it only discloses NPI to affiliates, if it shares certain information with its affiliates, it may have an obligation to provide an opt-out notice under the Fair Credit Reporting Act. That opt-out notice must be included in the firm's GLB privacy notice. (Click here to see **Fair Credit Reporting Act**).

Exercising the Opt-Out Right

The firm must give consumers and customers a reasonable opportunity to exercise their right to opt out—a period of 30 days, for example—after the firm sends the initial notice before the firm can share their information with nonaffiliated third parties outside the exceptions. For an isolated consumer transaction, like buying a money order, the firm may require its consumers to make their opt-out decision before completing the transaction.

Consumers and customers who have the right to opt out may do so at any time. Once the firm receives an opt-out direction from its existing consumers or customers, the firm must comply with it as soon as is reasonably possible.

The Shelf Life of an Opt-Out Direction

An opt-out direction by a consumer or customer is effective—even after the customer relationship is terminated—until the opt-out direction is canceled in writing, or, if the consumer agrees, electronically. However, if a former customer establishes a new customer relationship with the firm and it is required to provide an opt-out notice, the customer must make a new opt-out direction that will apply only to the new relationship.

Exceptions to the Notice and Opt-Out Requirements

There are a number of exceptions to the notice and opt-out requirements. These exceptions are located in sections 313.14 and 313.15 of the Privacy Rule and are referred to as section 14 and section 15 exceptions, respectively. If the firm shares information only under these sets of exceptions, it doesn't need to give its ***consumers*** a privacy notice; however, it will need to give its ***customers*** a simplified initial and, if applicable, an annual privacy notice. Customers and consumers have no right to opt out of these disclosures of NPI.

The section 14 exceptions apply to various types of information-sharing that are necessary for processing or administering a financial transaction requested or authorized by a consumer. In

contrast, the section 15 exceptions apply to certain types of information-sharing, including disclosures for purposes of preventing fraud, responding to judicial process or a subpoena, or complying with federal, state, or local laws.

Exception to the Opt-Out Requirement: Service Providers and Joint Marketing

Another exception can be found in section 313.13 of the Privacy Rule and is referred to similarly as the section 13 exception. If the firm shares information under this exception, it must give customers—and its consumers if the firm also shares their information—a privacy notice that describes this disclosure. However, neither the firm's consumers nor its customers have a right to opt out of this information sharing.

The section 13 exception covers disclosures for certain service providers and marketing activities whose services for the firm do not fall within the section 14 exceptions. For example, services not falling within the section 14 exceptions include:

- Services in connection with marketing the firm's products or marketing financial products jointly for the firm and another financial institution; or
- Services involving the performance of a general analysis of the firm's customer transactions.

Since the firm's disclosure of NPI for these purposes does not fall under the section 14 exceptions, the firm can use the section 13 exception for disclosure to them.

The section 13 exception also applies to marketing financial products or services offered through a joint agreement with one or more other financial institutions. The joint agreement requirement means that the firm has entered into a written contract with one or more financial institutions about the firm's joint offering, endorsement, or sponsorship of a financial product or service. This does not apply to all kinds of joint marketing engaged in by the firm; instead, it applies ***only*** to joint marketing with other financial institutions and ***only*** to the marketing of financial products or services.

To take advantage of the section 13 exception, the firm must enter into a contract with those nonaffiliated third parties with whom it shares NPI. The agreement must guarantee the confidentiality of the information by prohibiting the third party from using or disclosing the information for any purpose other than the one for which it was received.

Sarbanes-Oxley Act of 2002

The security of customer data is also addressed in the Sarbanes-Oxley Act of 2002. Section 404 requirements of the 2002 Act related to the safeguarding of customer information apply to all SEC-reporting companies with a market capitalization in excess of $75 million. It requires such companies to establish an infrastructure to protect and preserve records and data from destruction, loss, unauthorized alteration or other misuse. This infrastructure must ensure there is no room for unauthorized alteration of records vital to maintaining the integrity of the business processes.

Penalties for Unauthorized Disclosure or Use of Taxpayer Information

Penalties may be imposed for a tax preparer's failure to comply with applicable laws and regulations concerning the unauthorized disclosure or use of taxpayer information. Such penalties are authorized under:

- Code of Federal Regulations §301.7216.1; and
- Internal Revenue Code §6713.

The term "disclosure," as used in this case, means the act of making tax return information known to any person in any manner whatever. Let's briefly consider these statutes.

Code of Federal Regulations §301.7216.1

Code of Federal Regulations (CFR) provision §301.7216.1 imposes criminal penalties on any person engaged in the business of preparing or providing services in connection with the preparation of tax returns who knowingly or recklessly makes unauthorized disclosure or use of information furnished to them in connection with the preparation of an income tax return.

A violation of section 7216 is a misdemeanor, with a maximum penalty consisting of the costs of prosecution and:

- Up to one year imprisonment,
- A fine of not more than $1,000, or
- Both imprisonment and fine.

To the extent that a taxpayer's use of a hyperlink results in the transmission of tax return information, this transmission of tax return information is considered a disclosure by the tax return preparer and, if not authorized by regulation, is subject to criminal penalties under section 7216.

Internal Revenue Code §6713

Internal Revenue Code (IRC) §6713 imposes civil monetary penalties on the unauthorized disclosure or use of taxpayer information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns. It prescribes a related civil penalty for disclosures and uses that constitute a violation of section 7216.

The penalty for violating section 6713 is as follows:

- $250 for each prohibited disclosure or use,
- Up to a maximum of $10,000 for a calendar year.

Internal Revenue Procedure 2007-40

As discussed in Section 5.03 of Revenue Procedure 2007-40, the security of taxpayer accounts and personal information is a top priority for the Service. Accordingly, the Revenue Procedure requires Authorized IRS e-file Providers to have security systems in place to prevent the unauthorized access to taxpayer accounts and personal information by third parties. It also specifies that certain other violations are subject to penalties or sanctions specified in the Revenue Procedure, including violations of:

- The GLB Act and the rules and regulations promulgated by the FTC implementing it, and
- The non-disclosure rules contained in IRC sections 6713 and 7216 or their implementing regulations.

Preparer penalties that may be imposed under appropriate circumstances include, but are not limited to, those set forth in sections 6694, 6695, and 6713.

Summary

- The Safeguards Rule requires financial institutions, including tax preparers, to have measures in place to keep customer information secure.
- In addition to developing their own safeguards, tax preparers must take steps to ensure that their affiliates and service providers also safeguard customer information placed in their care.
- The objectives of the Safeguards Rule are to a) ensure customer record and information security and confidentiality, b) protect against anticipated threats/hazards to customer record security or integrity, and c) protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to the customer.
- The Safeguards Rule requires that financial institutions develop, implement and maintain a written and accessible Information Security Program.
- The Financial Privacy Rule aims to protect the privacy of the consumer by requiring tax preparers to give their customers privacy notices that explain their information collection and sharing practices.
- For purposes of the FTC's Privacy and Safeguards Rules, a "consumer" is someone who obtains or has obtained a financial product or service from a tax preparer that is to be used primarily for personal, family, or household purposes.
- A "customer," for purposes of the FTC's Privacy and Safeguards Rules, is a consumer who has a continuing relationship with the firm.
- All tax preparer's customers must be given an initial and annual privacy notice.
- If the tax preparer shares nonpublic personal information (NPI) with nonaffiliated third parties outside of specified exceptions, the firm also must give its customers an "opt-out" notice explaining the individual's right to direct the firm not to share her NPI with a nonaffiliated third party, a reasonable way to opt out and a reasonable amount of time to opt out.
- Before sharing NPI with nonaffiliated third parties outside of specified exceptions, the firm must give its non-customer consumers a privacy notice, including an opt-out notice.

- The privacy notice must include information concerning the categories of information collected, the categories of information disclosed and the categories of affiliates and nonaffiliated third parties to whom the firm discloses the information.
- The firm must deliver privacy notices in writing, or, if the consumer or customer agrees, electronically.
- The firm's written privacy notices may be delivered by mail or by hand.
- For individuals who conduct transactions with the firm electronically, the firm may post its privacy notice on its website and require them to acknowledge receiving the notice as a necessary part of obtaining a particular product or service.
- If the firm shares NPI with nonaffiliated third parties outside of specified exceptions, it must give consumers and customers an opt-out notice.
- The required opt-out notice must describe a way to opt out considered reasonable before the firm can disclose NPI to nonaffiliated third parties.
- The firm must provide a reasonable opportunity to exercise recipients' right to opt out before the firm can share NPI with nonaffiliated third parties outside specified exceptions.
- Criminal and civil penalties may be imposed for a tax preparer's failure to comply with requirements concerning the unauthorized disclosure or use of taxpayer information.
- Criminal penalties for a privacy violation have a maximum penalty consisting of the costs of prosecution and up to one year imprisonment, a fine of not more than $1,000, or both.
- Civil penalties of $250 for each prohibited disclosure or use, and up to a maximum of $10,000 for a calendar year.

Summary of Privacy Notice Requirements

TYPE OF NOTICE	TO WHOM	WHEN	CONTENTS
Initial	Customers	Not later than when you establish the customer relationship, unless it would substantially delay the transaction and the customer agrees	Description of information-collection and sharing practices, and opt-out notice (if you share NPI with nonaffiliated third parties outside of certain exceptions)
	Consumers who are not customers (including former customers)	Before you disclose their NPI to a nonaffiliated third party outside of certain exceptions	Full description of information-collection and sharing practices or "short-form" notice, along with opt-out notice
Annual	Customers	Delivery on a consistent basis at least once in any period of 12 consecutive months for the duration of the customer relationship	Description of information-collection and sharing practices, and opt-out notice (if you share NPI with nonaffiliated third parties outside of certain exceptions)

Chapter Review

1. The Jefferson Valley Tax Consulting company, a professional tax preparer, shares no client non-public personal information. Which of the following is correct as to its requirement to provide a privacy notice?

A. Since no non-public client information is shared, no privacy notice is required

B. Since no non-public client information is shared, a privacy notice needs to be sent only to the firm's consumers

C. A privacy notice is required to be sent to all clients, whether they are consumers or customers

D. Since no non-public client information is shared, a privacy notice is required to be furnished only to the firm's customers

2. If a tax preparer shares its customers' non-public information with a nonaffiliated third party, what must it, therefore, provide to them?

A. An opt-out notice

B. A reasonable stipend

C. An explanation of why the information-sharing is done

D. An explanation that a full privacy notice is available upon request

Chapter 3 – The Costs of a Data Breach

Introduction

An organization may experience a data breach that puts client information at risk from a range of causes including information technology or business process failures, human error or cyberattack. An organization experiencing a data breach needs to verify that a data breach occurred and, if so, how it happened. Once it has been determined that a data breach occurred, the organization's efforts generally become focused on remediation and on an attempt to minimize the short-term and long-term consequences of the breach on the firm and its clients. All those activities involve costs that may be direct, indirect or opportunity costs. This chapter will examine those activities and their financial impact on the firm.

Chapter Learning Objectives

When you have completed this chapter, you should be able to:

- List the principal causes of a data breach involving customer records;
- Identify the investigation and remediation activities normally undertaken by an organization following a data breach involving customer information;
- Recognize the average costs of a data breach in the United States; and
- Understand the probability of a business experiencing a data breach within the next 24 months.

Data Breach

A data breach is an event—either accidental or intentional—that discloses an individual's name and financial information and potentially puts that person at risk. Although a data breach can involve information in either or both paper and digital format, the increasing digitalization of data and the sophistication of cybercriminals results in a focus on computer-stored information and its security.

Causes of Data Breach

Although data breaches may result from many different causes, the principal causes of a data breach that compromises the records of clients and potentially puts their personal and business information at risk are:

- A criminal attack on a computer or network;
- Human error by an employee; and
- Business process or IT failures.

A compromised record is information that identifies the taxpayer whose information has been lost or stolen in a data breach.

Cybercrime Costs

In a white paper entitled "The Phishing Breakthrough Point," it is estimated that the annual global cost of cybercrime perpetrated in 2015 was $450 billion,[3] and a recent Forbes article[4] sees its average annual cost increasing to $6 trillion by 2021. More illuminating, however, is a study addressing the average cost of a data breach ***per compromised record.*** According to a 2017 study[5] commissioned by IBM and undertaken by the Ponemon Institute, LLC on the cost of a data breach, the average cost to a financial services organization—a category that includes professional tax preparers—for each compromised record was $245.

The costs included in the total and incurred by a company victimized by a data breach generally are the result of the necessary functions undertaken by the organization related to:

---

[3] https://info.knowbe4.com/whitepaper-phishing-breakthrough-point.
[4] https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#60628b854947.
[5] https://www.ibm.com/security/data-breach.

- Detection or discovery of the breach that requires the company to engage in activities to detect the breach of firm and/or taxpayer information;
- Escalation activities necessary to report the breach to appropriate organization personnel;
- Notification activities to inform affected taxpayers of the data breach by –
  - Letter,
  - Telephone call,
  - Email, or
  - General notice; and
- Post-data breach communications with taxpayers to help them minimize potential harms of the breach by offering –
  - Credit report monitoring, and/or
  - Assistance in reestablishing accounts or credit cards.

In addition to these activities, many companies experience opportunity costs—costs that may be even more damaging to the firm—resulting from diminished trust or confidence in the organization. Accordingly, such breaches involve:

1. Direct costs — the direct cash outlays to accomplish an activity, such as staffing a help desk;
2. Indirect costs — the expense related to the amount of time, effort and allocation of other organizational resources to identify and resolve the data breach; and
3. Opportunity cost — the loss of current clients and future business resulting from public disclosure of the breach.

Historically, even a single cyberattack can be enormously expensive and, according to Kaspersky Lab Research,[6] the average cost of a single data breach in a small to medium-size business is $117,000. For large firms, the average cost is $1.3 million.

IBM-Ponemon Study

The cited IBM-commissioned study included information from 419 companies headquartered in 11 countries and involved interviews with 1,900 individuals knowledgeable about the data breach in the organizations. The expenses considered in determining the average costs included only the expenses incurred in events directly relevant to the data breach, such as:

- Additional time required from the victim's staff;
- Fees charged by external consultants;
- Lost business; and
- Public relations costs to help overcome the damage to the firm's reputation.

The cost of a data breach is seen to vary depending on the country in which the business is headquartered and does business, the type of industry and the size of the breach and is affected by:

- The unanticipated customer loss following a data breach;
- The number of records lost or stolen;
- The amount of time it takes to identify and contain a data breach;
- The type of detection and data breach escalation involved;
- Whether the data breach is the result of a system glitch, employee negligence or a malicious attack perpetrated by a cyber criminal; and
- The costs incurred following the data breach.

Let's look more closely at the factors that affect an organization's cost of a data breach.

Customer Loss

There is little question about the value of an existing customer. Every business person knows that keeping existing customers is a far more efficient and less costly way of growing a business than constantly needing to find and attract new customers. A business's inability to keep its existing customers has serious short-term and long-term financial consequences.

[6] https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-research-shows-ddos-devastation-on-organizations-continues-to-climb.

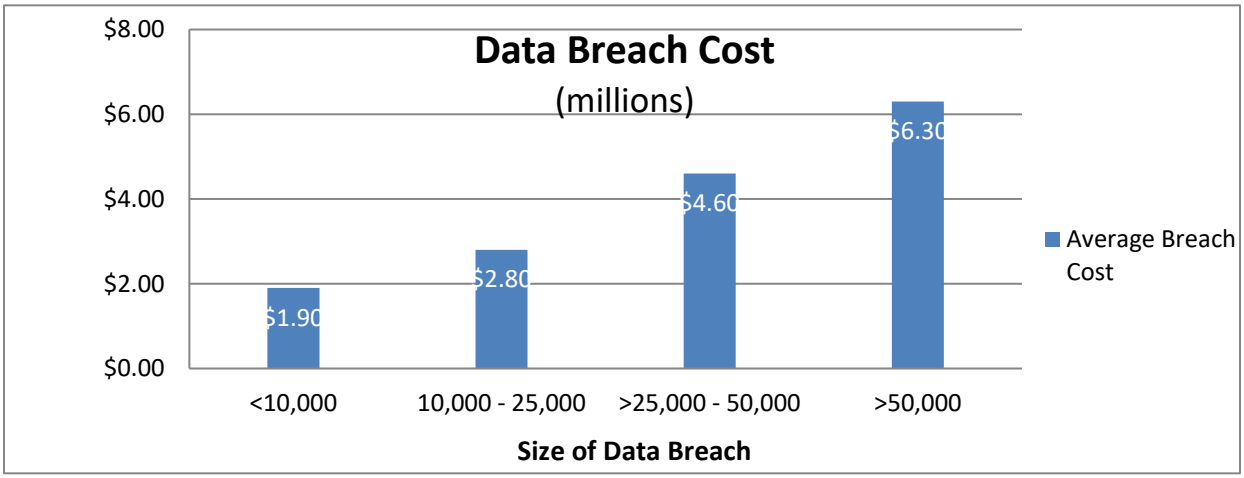
An interviewed business that lost less than one percent of its customers following a data breach had an average total data breach cost of $2.6 million. If the loss of customers increased to 4% or more, the average aggregate cost of the data breach grew to $5.1 million. Businesses experiencing the largest customer loss—presumably because of the more sensitive nature of the compromised customer data—were those in the financial and health industries. Furthermore, United States business organizations experienced the highest cost of losing customers at an average of $4.13 million.

Businesses that implement programs designed to preserve and enhance customer trust and loyalty *before any data breach occurs* are expected to be able to reduce the number of lost customers if the breach occurs specifically because of that enhanced trust and consequent loyalty. One of the principal methods businesses can implement to help preserve and enhance customer trust is to employ a senior-level leader—typically referred to as a *chief privacy officer* or *chief information security officer*—whose function is to direct initiatives that improve customers' trust in how the organization safeguards their personal information. By implementing such a program, businesses can expect to reduce the loss of business following a data breach as well as the overall cost of the breach.

Number of Records Stolen or Compromised

There is a clear and unsurprising relationship between the size of a data breach and its average total cost to the victimized business; specifically, the larger the amount of data lost, the greater the cost incurred by a business experiencing a breach. Since a firm's document-retention program is a major factor in the size of any potential breach and its cost, a firm that retains only the data that must be retained to comply with IRS and other regulations can reduce the cost to remediate a data breach if and when it occurs.

Of the organizations included in the IBM study, those in the United States were among the firms experiencing the largest average number of compromised records. As shown in the graph below, the cost ranged from $1.9 million for data breaches involving fewer than 10,000 compromised records to $6.3 million for data breaches involving more than 50,000 compromised records.



Time Required to Identify and Contain a Data Breach

A firm's cost in dealing with a data breach is affected significantly by how long it takes the organization to identify a breach and contain it. A firm's inability to quickly identify the data breach increases the costs it incurs.

Those firms in the IBM study with a median time to identify the data breach of fewer than 100 days incurred an estimated average total cost of the data breach of $2.8 million, while those organizations having a median time of more than 100 days to identify the breach had an estimated average total cost of $3.83 million. The difference in cost that varies based on the duration of time between the attack and its detection suggests that the inability to quickly

identify the data breach leads to higher costs. For that reason, it would seem clear that an organization's possession of tools and methods that improve detection capabilities—specifically, forensic and investigative tools—can significantly reduce data breach cost.

The costs incurred in identifying a data breach generally include the expenses involved in:

- Forensic and discovery-related activities, including conducting investigations and forensics to determine the root cause of the data breach;
- Assessment and audit services including determining the probable victims of the data breach;
- Crisis team management that includes organizing an incident response team; and
- Communications to executive management and board of directors.

The average cost of detection and escalation incurred by the U.S. firms in the IBM study was $1.07 million. An organization's investment in governance, risk management and compliance programs that improve its ability to detect and contain a data breach can reduce the time involved in identifying and containing the breach and, as a result, its costs to do so.

Cause of the Data Breach

Whether a data breach is the result of human error, a system glitch or a malicious attack also impacts the median time to identify and then contain the breach. As a result, costs incurred in dealing with the breach vary, depending on the cause.

For the three principal causes of a data breach incident—human error, system glitch or malicious attack—the median time needed to identify that an attack occurred and the median time needed to contain a malicious or criminal attack was the highest at 214 days and 77 days, respectively. For data breaches occurring as a result of human error or system glitch, the durations before identification and containment are much lower at approximately 168 and 54 days, respectively.

The study showed that when the root cause of the data breach was a malicious or criminal attack, the average cost for each file compromised was greater than if the cause was a system glitch or human error. Factors that may decrease the cost are participation in threat sharing, use of security analytics and the recruitment and retention of knowledgeable personnel.

Remediation and Other Costs Following Identification of Breach

After a data breach is discovered, the organization must determine what is needed in order to provide appropriate services to taxpayers affected by the breach and to limit the organization's liability. Costs are incurred to purchase and/or provide the services generally needed to handle those requirements following a breach.

The typical activities conducted in the aftermath of discovery of a data breach include:

- Engaging audit and consulting services to help determine the cause and extent of the breach;
- Engaging legal services for –
    - Defense against client lawsuits, and
    - Representation concerning compliance;
- Providing for and offering free or discounted identity protection and other services to victims of the data breach;
- Conducting communication/public relations outreach to affected taxpayers and implementing call center procedures;
- Preparing notice documents and other required disclosures to data breach victims and regulators; and
- Staffing a help desk and implementing specialized training to handle additional inbound telephone and written communications.

As noted earlier, in addition to the direct costs involved in these activities, firms normally experience the opportunity costs resulting from lost business.

Purchasing insurance to compensate for some or all the costs of a data breach can help manage the financial consequences of the incident. However, certain things can increase the costs of a breach, including:

- An organization's rush to notify victims without a thorough understanding of the scope of the breach;
- Compliance failures; and
- The engagement of consultants.

Probability of Experiencing a Data Breach

It is fair to conclude, based on the IBM report, that a data breach is expensive for the firm experiencing it. But, how likely is it that a data breach will occur at any particular organization? According to the IBM-Ponemon study cited earlier, the probability of a material data breach occurring at any organization over the next 24-month period is estimated to be 26.8%—an increase from the previous year of approximately 4%.

Summary

- A data breach is an event—either accidental or intentional—that discloses an individual's personal and/or financial information and potentially puts the taxpayer at risk of some type of loss.
- The principal causes of a data breach that compromises records and potentially puts clients' personal and business information at risk are:
    - Criminal attacks,
    - Human error by an employee, and
    - Business process or IT failures.
- The average cost to a financial institution—a category that includes a professional tax preparer organization—for each compromised record in 2016 was $245.
- The average cost of detection and escalation incurred by the U.S. firms following a material data breach in 2016 was $1.07 million.
- Factors that may decrease the cost of a data breach include:
    - Participation in threat sharing,
    - Use of security analytics, and
    - The recruitment and retention of knowledgeable personnel.
- The probability of a material data breach occurring at any organization over the next 24-month period is estimated to be 26.8%.

Chapter Review

1. What is the average cost per compromised record of a data breach to a financial institution according to a 2017 IBM study?

    A. $137

    B. $245

    C. $376

    D. $483

2. How likely is it that a firm will suffer a material data breach over the next 24-month period as estimated in the 2017 IBM study?

    A. 9.4%

    B. 17.3%

    C. 26.8%

    D. 37.9%

Chapter 4 – The Information Security Plan

Introduction

As discussed earlier, although a data breach is not inevitable, approximately one in four organizations is likely to experience such a breach involving the compromise of client data within the next 24 months. The average cost incurred by a financial services organization following a data breach is $245 per compromised record; overall, the average cost of a data breach—solely for detection and escalation—experienced by U.S. companies is $1.07 million. When the additional expenses associated with remediation, etc. are added, the average costs are considerably higher.

Data breaches generally are caused by human error, an information technology (IT) or business process failure, or a cyberattack. An important defense against the occurrence of a data breach involves the creation and maintenance of a firm's written Information Security Plan and its rigorous implementation. This chapter will examine the elements of such a plan and the necessary steps to create one.

Chapter Learning Objectives

When you have completed this chapter, you should be able to:

- Recognize the function of a firm's Information Security Plan;
- List the principal sections of an Information Security Plan;
- Identify the role of an Information Security Plan's physical security procedures; and
- Describe the elements comprising a firm's information and computer system.

Ensuring Data Security

Making sure taxpayer data and other firm information is secure can be vitally important. As noted in the previous chapter, the average cost of a data breach experienced by a small to medium size company was $117,000.

Although it is probably impossible to protect an ongoing business enterprise from every potential data breach short of closing its doors, certain steps can be taken to reduce the risk to its data. However, helping to ensure that a firm's data is secure requires the firm and its management to seriously address it beginning with its policies and procedures.

While the terms "policies" and "procedures" are sometimes seen as referencing the same thing, they are not identical. Instead, policies are high level, simple guides charting an organization's course and pointing it in a specific direction. In contrast to the simplicity of policies, procedures are far more detailed and act as step-by-step guides on how to bring about the results envisioned in the policies.

Accordingly, a procedure spells out:

- What is to be done,
- Who does what,
- How it is to be done,
- When it is to be done,
- What a good result looks like, and
- How to fix non-conformance.

In short, while a policy points the organization in a specific direction, a procedure tells it the path to follow to get there, how to follow it and ultimately to understand when it has arrived at its destination. Whether the firm is a one-person organization or employs thousands, it should institute a policy helping to ensure the safety of its taxpayer data and identify the appropriate procedures to:

- Identify an individual to be responsible for data safeguards;
- Assess the firm's risk that its data will be compromised;
- Write a plan—generally referred to as its Information Security Plan—detailing how the firm will safeguard its taxpayer information;
- Implement the Information Security Plan;

- Monitor and evaluate the Information Security Plan periodically and whenever the business or the circumstances change; and
- Adjust the firm's Information Security Plan in response to ongoing identified risks.

Let's consider each of these steps.

Where to Begin: Determining Responsibility

A simple truth resides in the principle that "nobody is responsible if everyone is responsible." In short, although every employee in the firm needs to help ensure the firm is protected against data breaches, one individual should normally have ***primary responsibility*** for the firm's data security. So, before any other cybersecurity task is undertaken, decide which individual will be responsible for:

- Overseeing data security;
- Ensuring the implementation of the cybersecurity plans decided on by the firm; and
- Monitoring data security effectiveness.

The individual identified as having primary responsibility for the firm's data security should report to senior management and/or the Board of Directors periodically as to the effectiveness of the firm's Information Security Plan and potential future data security risks.

Identifying the Risks and Their Impact

Clearly, in order to create an appropriate Information Security Plan for the firm, the firm and its senior management must be aware of the risks of a data breach and the potential impact on the firm and its clients of the data's unauthorized:

- Access;
- Use;
- Disclosure;
- Modification; or
- Destruction.

Thus, the firm needs to complete a thoroughgoing risk assessment that, at the very least, addresses the following questions:

- How vulnerable is the firm's customers' data to theft, disclosure, unauthorized alterations or unrecoverable loss?
- What can the firm do to reduce the impact to its customers and the business in the event a data breach occurs?
- What can the firm do to reduce its vulnerability?

Writing an Information Security Plan

Once the risks of a data breach have been assessed and the impact of such a breach on the firm and its clients has been determined, the next important step is to write an Information Security Plan to help ensure the security of the firm's data. Although several individuals may be responsible for the plan's development and implementation, it should identify and name the one person having primary responsibility for the firm's data security. Additionally, it should:

- Address each item the firm has identified in its risk assessment;
- Define the safeguards the firm wants affiliates and service providers to follow;
- Require a responsible member of the firm's management to –
    - Review and approve the plan,
    - Monitor and test the plan periodically,
    - Revise the plan as needed to address any identified problems or business changes; and
- Provide for a periodic self-assessment to –
    - Evaluate and test the plan and other safeguards the firm has in place, and
    - Document and address any identified safeguard deficiencies.

In addition to writing the Information Security Plan, the firm should also do the following:

- Retain a copy of the periodic self-assessments and ensure they are available for any potential reviews by management and/or authorities;

- Provide notices of the firm's privacy practices to its customers and, if required by the FTC privacy rule, to consumers;
- Specify in contracts with its service providers the privacy safeguards they are required to follow and monitor their handling of taxpayer information; and
- Obtain a copy of service providers' written policy on safeguarding information.

The firm's Information Security Plan should be created with both specificity and flexibility so that—if followed—it will reduce the firm's vulnerability to a cyberattack or other potential danger to its data by addressing:

- Security of the physical facility;
- Personnel security;
- Information and computer systems security; and
- Media security.

Let's consider each of these areas of potential vulnerability to attack.

Securing the Physical Facility

The "physical facility" whose security must be addressed in the firm's Information Security Plan includes the office in which client files can be accessed and storage facilities housing any files, whether paper or digital. It also includes:

- Each PC and computer laptop used for accessing or storing taxpayer information;
- The central computer room, if such exists; and
- The delivery and removal of taxpayer information.

Accordingly, the physical facility part of the plan should address and accomplish the following:

- Protect all places where taxpayer information is located from unauthorized access and potential danger, such as destruction from –
    - Theft,
    - Fire,
    - Hurricanes,
    - Floods and
    - Tornados;
- Prevent unauthorized access and unauthorized processes (even by persons whose access is authorized);
- Assure that taxpayer information, including data on hardware and media, is not left un-secured where unauthorized access can occur, such as –
    - On desks or photocopiers,
    - In mailboxes, vehicles, trash cans or rooms in the office, or
    - At home;
- Authorize and control delivery and removal of all taxpayer information, including data on hardware and media;
- Require that the doors to file rooms and/or computer rooms be locked at all times; and
- Provide secure disposal of taxpayer information, via –
    - Shredders,
    - Burn boxes, or
    - Temporary file areas.

Personnel Security

Personnel security involves the protection of firm and taxpayer data from compromise and/or loss as a result of use or misuse by firm employees or former employees. Accordingly, a firm's Information Security Plan needs to address:

- Human error resulting from ignorance or fatigue; and
- Intentional unauthorized access.

Protection of Data from Human Error

Taxpayer and firm data are at risk of loss or compromise from human errors made by employees principally as a result of two conditions:

1. Ignorance of appropriate rules of behavior with respect to confidential data; and
2. The normal fatigue that often accompanies characteristically-extended employee work hours during tax time.

Although it is unlikely that data loss or compromise resulting from human error caused by ignorance will ever be completely eradicated, the firm's Information Security Plan can go a long way to reducing it by including:

- Rules of Behavior that describe responsibilities and expected behavior regarding taxpayer and firm data in connection with –
  - Computer information systems,
  - Paper records, and
  - Usage;
- The requirement for written and signed employee acknowledgment that they have read, understood and agreed to comply with the firm's Rules of Behavior; (See sample Rules of Behavior in the Appendix 1)
- An explanation of the Rules of Behavior employees are expected to follow when interviewing prospective personnel;
- A requirement for –
  - Background and/or reference checks on new employees who will have contact with taxpayer information,
  - Background screenings of new and prospective employees that are appropriate to the sensitivity of the assigned position, and
  - Screening of personnel prior to granting access to any paper or electronic data to help ensure their suitability for a position requiring confidentiality and trust;
- Creation and enforcement of formal compliance policies and processes, including possible disciplinary action for personnel who do not comply with the firm's established information security policies and procedures;
- The requirement that personnel from third-party providers such as service bureaus, contractors, and other businesses providing information technology services to the firm meet the same security requirements as those applied to the firm's personnel; and
- The stated requirement that –
  - Staff be trained on rules of behavior concerning access to, nondisclosure of and required safeguards of taxpayer and firm information, and
  - Refresher training takes place periodically.

Protection of Data from Intentional Compromise or Loss

Although taxpayer and firm data certainly may be compromised or lost as a result of employees' unintentional failure to take appropriate precautions, the more sinister and costly cause is a cyberattack mounted by someone intent on stealing company and taxpayer information.

To reduce the probability of a cyberattack by a current or former employee, the firm's Information Security Plan should require (in addition to the material discussed immediately above) that:

- Nondisclosure agreements be signed by any personnel who will have access to confidential taxpayer or firm proprietary information;
- Access to taxpayer information (e.g., login IDs and passwords) be immediately stopped for those employees who are terminated or who no longer need access; and
- An exit interview be conducted with each terminated employee during which all property that allows access to taxpayer information (e.g., laptops, media, keys, identification cards and building passes) be returned to the firm.

Information and Computer Systems Security

The term "information systems" refers broadly to the many activities involving information engaged in by the firm and its employees. It includes automated and manual systems that are comprised of people, machines and/or methods for data:

- Collection;
- Processing;
- Transmission;
- Storage;

- Archiving; and
- Distribution.

The firm's Information Security Plan, with respect to information and computer systems security, should contain written policies and procedures:

- Granting access to taxpayer and firm information systems to employees only to satisfy a valid business need determined by the individual's role within the firm;
- Detailing a contingency plan to enable the firm to perform critical processing in the event business is disrupted; such a plan includes –
    - Plans to protect electronic and paper taxpayer information,
    - Identification of individuals responsible for data recovery and restoration of the system after failure or disruption, and
    - Periodic testing of the contingency plan;
- Requiring regular backing up of taxpayer data files and storage of backed-up information in a secure location;
- Concerning the maintenance of hardware and software as needed (and requiring that maintenance records be kept);
- Addressing the identification and authentication of computer system users who require access to electronically-maintained taxpayer information systems before granting them access by –
    - Identifying authorized users and granting specific access rights/privileges,
    - Assigning each user a unique identifier,
    - Verifying the identity of each user before permitting access,
    - Disabling user identifiers after an organization-defined time period of inactivity, and
    - Archiving current and disabled user identities;
- Requiring the implementation of password management procedures that ensure use of strong passwords –
    - Comprised of 8 - 16 characters, and
    - Containing a combination of numbers, symbols, uppercase letters, lowercase letters, and spaces;
- Mandating periodic password changes based on the firm's determination of the importance of the data (the more important the information, the more frequent the required changes);
- Requiring that disabled and inactive user accounts be removed;
- Requiring that electronic taxpayer information systems connected to the Internet be protected with a barrier device (e.g., firewall, router or gateway) to avoid unauthorized release of taxpayer data;
- Identifying and requiring the use of best practices when storing taxpayer information electronically;
- Calling for the storage of taxpayer information on separate password-protected and encrypted secure computers or on media unconnected to a network;
- Requiring encryption of taxpayer information when –
    - Attached to email, or
    - Transmitting across networks;
- Requiring regular updating of firewall, intrusion detection, anti-spyware, anti-adware, anti-virus software and security patches;
- Concerning the monitoring of computer systems for unauthorized access by reviewing system logs;
- Requiring the lock-out of computer system users after three consecutive invalid access attempts;
- Authorizing and requiring removal of all taxpayer information once the retention period expires by using software designed to securely remove data from computers and media prior to disposing of hardware or media (the FTC Disposal Rule should be followed to dispose of sensitive data); and
- Requiring the performance of vulnerability scans and penetration tests periodically to reduce computer system risks. (See FTC article "FTC Facts for Business - Security Check: Reducing Risks to Your Computer Systems.")

Media Security

The term "media," as used in connection with information security, refers to any method of presenting and/or storing information. It encompasses computer disks, tapes, compact disks, flash drives, audio and video recordings, and paper documents. The firm's Information Security Plan should also address media and require that:

- Taxpayer information be stored in a secure location, cabinet, or container, regardless of whether stored on –
  - Computer disks,
  - Removable media,
  - Tapes,
  - Compact disks,
  - Flash drives,
  - Audio and video recordings of conversations and meetings with taxpayers, or
  - Paper documents;
- Media storage areas, including rooms, cabinets, and computers be secured by locks or key access;
- Authorized access to media storage be restricted, and, where appropriate, an automated mechanism be employed to ensure only authorized access;
- Removal of taxpayer information be limited only to authorized persons;
- Information access audits be performed regularly;
- All taxpayer information be securely removed (as provided by the FTC Disposal Rule) when disposing of computers, diskettes, magnetic tapes, hard drives, or any other electronic media that contain taxpayer information; and
- All paper documents be shredded or burned before being discarded.

Summary

- To comply with applicable legal requirements, firms must have policies and procedures to combat data breaches.
- Policies point the direction an organization's management chooses to take it.
- Procedures spell out what is to be done, who does what, how it is to be done, when it is to be done, what a good result looks like, and how to fix non-conformance.
- A single individual should normally be identified as having the responsibility for ensuring the firm is protected against data breaches.
- The firm's Information Security Plan contains the procedures for addressing the security of the physical facility, personnel security, information and computer systems security and media security.
- Procedures directed at ensuring physical security are designed to protect taxpayer and firm data from destruction by natural means—fire, flood, etc.—as well as offering protection against unauthorized access.
- Personnel security procedures include Rules of Behavior that describe personnel responsibilities and expected behavior regarding taxpayer and firm data.
- Information and computer system security addresses the security of automated and manual systems that are comprised of people, machines and/or methods for the collection, processing, transmission, storage, archiving and distribution of firm and taxpayer data.
- Media security is designed to help ensure the security of computer disks, removable media, tapes, compact disks, flash drives, audio and video recordings, and paper documents containing firm and taxpayer data.

Chapter Review

1. Which of the following is NOT recommended for reducing the probability of a cyberattack by current and/or former employees?

   A. The requirement that employees having access to taxpayer information sign nondisclosure agreements

   B. Revoking access to taxpayer information by employees who terminate or no longer need access

C. Retrieval of all property enabling access to taxpayer information from terminating employees during an exit interview

D. Immediately escorting terminating employees out of the firm's premises

2. Which of the following data breaches is usually considered the costliest for tax preparers that have been victimized?

A. The loss of taxpayer data due to employee negligence

B. Theft of taxpayer data resulting from a cyberattack

C. Compromise of taxpayer data as a result of employee ignorance

D. Loss of taxpayer data due to a business process glitch

Chapter 5 – Best Practices for Securing Data

Introduction

Tax preparers normally have access to sensitive taxpayer financial information they are required to safeguard from unauthorized access. This chapter discusses the best practices tax preparers may employ to detect and avoid unauthorized intrusion of their information systems and addresses measures that may be taken to help ensure such avoidance in the areas of:

- Employee management and training;
- Firm policies and procedures; and
- Information system security.

Chapter Learning Objectives

When you have completed this chapter, you should be able to:

- List the data use and retention areas generally vulnerable to unauthorized access of taxpayer information; and
- Identify best practices for securing taxpayer information.

Recommended Practices

The FTC recommends that firms consider implementing various best practices appropriate for the nature of their business operations that are designed to help safeguard taxpayer and other customer information. The suggested best practices include those related to:

- Employee management;
- Employee training;
- Firm policies and procedures; and
- Information system security.

Let's consider each of these recommended practices.

Employee Management

The success of a firm depends largely on its employees; that principle also applies to data security and the employees who implement it. Tax preparers are urged to consider:

- Checking references or doing background checks before hiring employees who will have access to customer information.
- Asking every new employee to sign an agreement to follow the firm's confidentiality and security standards for handling customer information.
- Limiting access to customer information to those employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.
- Controlling access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (Strong, tough-to-crack passwords require the use of at least eight characters consisting of a combination of upper- and lower-case letters, numbers, and symbols.)
- Using password-activated screen savers to lock employee computers after a period of inactivity.
- Developing policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device.

Employee Training

It isn't surprising that, since the majority of data breaches occur as the result of the confidence scam known as phishing, a large part of any firm's avoidance of cybercrime begins with employee training.

Maintaining the security, confidentiality, and integrity of customer information involves training employees to take basic steps to help ensure that happens. Those basic data-safety steps include:

- Locking rooms and file cabinets where records are kept;
- Not sharing or openly posting employee passwords in work areas;
- Encrypting sensitive customer information when it is transmitted electronically via public networks;
- Referring calls or other requests for customer information to designated individuals who have been trained in how the company safeguards its personal and taxpayer data;
- Reporting suspicious attempts to obtain customer information to designated personnel; and
- Regularly reminding all employees of the company's policy—and the legal requirement—to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.

Policies and Procedures

The policies and procedures adopted by any firm are the "rules of the road" that inform employees of the firm's expectations. With respect to data security, firms should consider:

- Developing policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.
- Imposing disciplinary measures for security policy violations.
- Preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.

Maintaining Information System Security

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some suggestions on maintaining security throughout the life cycle of customer information, from data entry to data disposal. Consider implementing FTC-suggested data safety measures, relating to:

- Information storage;
- Controls to prevent unauthorized system access;
- Customer data transmission;
- Disposal of customer data;

Information Storage

Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example:

- Ensure that information storage areas are protected against destruction or damage from physical hazards, such as fire or floods.
- Store records in a room or cabinet that is locked when unattended.
- When customer information is stored on a server or other computer, ensure that the computer is accessible only with a "strong" password and is kept in a physically-secure area.
- Where possible, avoid storing sensitive customer data on a computer with an Internet connection.
- Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area.
- Maintain a careful inventory of the company's computers and any other equipment on which customer information may be stored.

Protecting against Unauthorized System Access

Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. To implement this best practice, be sure to:

- Check with software vendors regularly to get and install patches that resolve software vulnerabilities;
- Use anti-virus and anti-spyware software that updates automatically;
- Maintain up-to-date firewalls, particularly if the firm uses a broadband Internet connection or allows employees to connect to the firm's network from home or other off-site locations;
- Regularly ensure that ports not used for the firm's business are closed; and
- Promptly pass along information and instructions to employees regarding any new security risks or possible breaches.

Detecting Possible Improper Disclosure

Effective security management requires the company to deter, detect, and defend against security breaches. Firms must take reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively. There is no absolutely-secure system that will enable a business to avoid all data breaches. For that reason, firms need to use appropriate oversight or audit procedures to detect any improper disclosure or theft of customer information.

The best practices to enable a firm to detect data breaches involving customer information include:

- Keeping logs of activity on the firm's network and monitoring them for signs of unauthorized access to customer information;
- Using an up-to-date intrusion detection system to alert the firm's management of attacks;
- Monitoring both inbound and outbound transfers of information for indications of a compromise, such as the unexpected transmission of large amounts of data from the firm's system to an unknown user; and
- Inserting a dummy account into each of the firm's customer lists and monitoring the account to detect any unauthorized contacts or charges.

To help avoid potential threats to taxpayer information, monitor the websites of the firm's software vendors and read relevant industry publications for news about emerging threats and available defenses.

Customer Data Transmission

Take steps to ensure that the transmission of customer information is accomplished securely. For example:

- When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit.
- If you collect information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message.
- If you must transmit sensitive data by email over the Internet, be sure to encrypt the data.

Disposal of Customer Information

Dispose of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule. For example:

- Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If the firm hires an outside disposal company, conduct due diligence beforehand by checking references and/or requiring that the company be certified by a recognized industry group.
- Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed.
- Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.

Summary

Suggested best practices to help detect and defend against data breaches address:

- Employee management and training, firm policies and procedures, and information system security.
- Background checks and new employee agreement to follow the firm's confidentiality and security standards.
- Controlling and limiting access to customer information to employees with a valid business reason to access it.
- Using password-activated screen savers to lock employee computers after a period of inactivity.
- Maintaining appropriate policies for use and protection of laptops and other devices.
- Locking rooms and file cabinets where records are kept.
- Not sharing or openly posting employee passwords in work areas.
- Encrypting sensitive customer information when transmitted electronically.
- Referring requests for customer information to designated, trained individuals.
- Reporting suspicious attempts to obtain customer information to designated personnel.
- Developing policies for employees who telecommute.
- Imposing disciplinary measures for security policy violations.
- Immediately deactivating passwords to prevent terminated employees from accessing customer information.
- Ensuring that information storage areas are protected from floods, earthquakes, etc.
- Locking cabinets and unattended rooms storing records.
- Mandating use of strong passwords to access customer information.
- Maintaining digital and other data in a physically-secure area.
- Not storing sensitive customer data on a computer with an Internet connection.
- Backing up records and storing offline in a physically-secure area.
- Maintaining a careful inventory of the company's computers and other equipment warehousing customer information.
- Obtaining and installing patches that resolve software vulnerabilities.
- Using automatically-updated anti-virus and anti-spyware software.
- Maintaining up-to-date firewalls.
- Closing computer system ports not used for the firm's business.
- Passing along timely information and instructions to employees regarding new security risks or possible breaches.
- Maintaining and monitoring logs of network activity.
- Using up-to-date intrusion detection system to alert management of attacks.
- Monitoring information transfers for indications of a compromise.
- Monitoring a dummy account for unauthorized contacts or charges.
- Transmitting sensitive financial data using a Secure Sockets Layer (SSL) connection.
- Transmitting sensitive data by email over the Internet only if encrypted.
- Designating a records retention manager to supervise disposal of records containing customer information.
- Conducting appropriate due diligence on hired records-disposal vendors.
- Burning, pulverizing, or shredding papers containing customer information.
- Destroying or erasing data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.

Chapter Review

1. In order to help reduce the chances of a data breach compromising taxpayer information, tax preparer firms should generally limit access to taxpayer information to

   A. firm executives

   B. all full-time employees

   C. CPAs

   D. employees having a business reason to access taxpayer information

2. As a way to help ensure the security of customer data, which of the following should normally be implemented?

A. Avoid storing sensitive customer information on a computer with an Internet connection
B. Grant access to sensitive customer information only through an easily-remembered password
C. Keep backup records secure by storing them online
D. Never encrypt customer data

Chapter 6 – When a Data Breach Occurs

Introduction

Given sufficient time and an increasing amount of business, it almost seems inevitable that a business housing taxpayer personal and financial data will suffer a data breach. While that statement isn't literally true, the risk that any firm will be attacked is significant. This chapter addresses what needs to be done when the breach occurs at your firm.

Chapter Learning Objectives

When you have completed this chapter, you should be able to:

- Identify the steps that should be taken by a business to stop or limit additional data loss if a data breach has occurred involving its clients;
- Recognize the need for a comprehensive communications plan;
- List the entities that should be notified in the event of a data breach; and
- Identify the additional protections that may be recommended if a data breach involves the compromise of clients' Social Security numbers.

When a Data Breach Occurs

In light of the cybercrime statistics as well as the increasing sophistication and reach of cyber criminals, the chance that any firm will be a victim of cyber crime is fairly high. Accordingly, all firms should take steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach.

If a breach occurs the firm should:

- Preserve customer data by –
    - Taking immediate action to secure any information that has been or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet to avoid any further data theft;
    - Preserving and reviewing files or programs that may reveal how the breach occurred; and
    - Bringing in security professionals if feasible and appropriate to help assess the breach as soon as possible.
- Consider notifying consumers, law enforcement, and/or businesses in the event of a security breach and:
    - Notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm;
    - Notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm;
    - Notify the credit bureaus and other businesses that may be affected by the breach; and
    - Determine if breach notification is required under applicable state law.

Secure the Firm's Operations

If a data breach occurs, management needs to move quickly to secure the firm's systems and fix vulnerabilities that may have caused the breach. Few things are worse than a data breach. However, multiple data breaches definitely are. Take immediate steps so it doesn't happen again. Mobilize the firm's breach response team right away to prevent additional data loss. The exact steps to take depend on the nature of the breach and the structure of the firm's business.

Assemble a team of experts to conduct a comprehensive breach response. Depending on the size and nature of the company, such a team may include management and experts in forensics, legal, information security, information technology, operations, human resources, communications, and investor relations.

- Identify a data forensics team and consider hiring independent forensic investigators to help determine the source and scope of the breach. Expect forensic experts to –
    - Capture forensic images of affected systems,
    - Collect and analyze evidence, and
    - Outline remediation steps;
- Talk to the firm's legal counsel. Then, consider hiring outside legal counsel with privacy and data security expertise to advise on federal and state laws that may be implicated by a breach.
- Secure physical areas potentially related to the breach. Lock them and change access codes, if needed. Ask forensics experts and law enforcement when it is reasonable to resume regular operations.
- Stop additional data loss and take the following steps –
    - Take all affected equipment offline immediately, but don't turn any machines off until forensic experts arrive,
    - Closely monitor all entry and exit points, especially those involved in the breach,
    - Put clean machines online in place of affected ones, if possible, and
    - Update credentials and passwords of authorized users. (If a hacker stole credentials, the firm's system will remain vulnerable until the firm changes them, even if the hacker's tools have been removed.

Remove Improperly Posted Information from the Web

Information can remain in cyberspace until it is removed. Take the following steps to help ensure improperly posted information doesn't continue to be available:

- If the data breach involved personal information improperly posted on the firm's website, immediately remove it. Be aware that Internet search engines store, or "cache," information for a period of time. Contact the search engines to ensure they don't archive personal information posted in error; and
- Search for the company's exposed data to make sure that no other websites have saved a copy. If any exposed data is identified, contact those sites and ask them to remove it.

Interview

Talk with the people who discovered the breach and anyone else who may know about it. If the firm has a customer service center, make sure the staff knows where to forward information that may aid the investigation of the breach. Be sure to document the firm's investigation but don't destroy any forensic evidence in the course of the firm's investigation and remediation.

Fix Vulnerabilities

When the investigation of the data breach is underway, the executive principally involved in data breach remediation should ensure the vulnerabilities that caused or may have led to the breach are fixed, including:

- Addressing the firm's service providers;
- Considering the firm's network segmentation; and
- Working with forensics experts.

Thinking about Service Providers

If service providers were involved, examine what personal information they can access and decide if you need to change their access privileges. Also, ensure the firm's service providers are taking the necessary steps to make sure another breach does not occur. If the firm's service providers say they have remedied vulnerabilities, verify that they really fixed things.

Checking the Firm's Network Segmentation

When the firm's network was established, it may have been segmented so that a breach on one server or in one site could not lead to a breach on another server or site. Work with forensics experts to analyze whether the firm's segmentation plan, if any, was effective in containing the breach. If any changes are required, do so now.

Working with Forensics Experts

Find out if measures such as encryption were enabled when the breach happened. Analyze backup or preserved data. Review logs to determine who had access to the data at the time of the breach. Also, analyze who currently has access, determine whether that access is needed, and restrict access if it is not. Verify the types of information compromised, the number of people affected, and whether the firm has contact information for those people. When the forensic reports are received, take the recommended remedial measures as soon as possible.

The Firm's Communications Plan

Create a comprehensive plan that reaches all affected audiences, including employees, customers, investors, business partners, and other stakeholders. Don't make misleading statements about the breach. And don't withhold key details that might help those affected by the breach to protect themselves and their information. Also, don't publicly share information that might put consumers at further risk.

Anticipate questions that people will ask. Then, put top tier questions and clear, plain-language answers on the firm's website where they are easy to find. Good communication up front can limit customers' concerns and frustration, saving the company time and money later.

Notify Appropriate Parties

When the business experiences a data breach, notify law enforcement, other affected businesses, and affected individuals.

Most states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. In addition, depending on the types of information involved in the breach, there may be other laws or regulations that apply to the firm's situation. Check state and federal laws or regulations for any specific requirements applicable to the business.

Notify Law Enforcement

Call the local police department immediately. Report the situation and the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective they can be. If the local police aren't familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service. For incidents involving mail theft, contact the U.S. Postal Inspection Service.

Notify Affected Businesses

If account access information—credit card or bank account numbers, for example—has been stolen, notify the institution that maintains the accounts so it can monitor the accounts for fraudulent activity.

If the firm collects or stores personal information on behalf of other businesses, notify them of the data breach. If names and Social Security numbers have been stolen, contact the major credit bureaus for additional information or advice. For a compromise involving a large group of people, advise the credit bureaus if you are recommending that people request fraud alerts and credit freezes for their files. The major credit bureaus and their contact information are:

- Equifax: equifax.com or 1-800-525-6285
- Experian: experian.com or 1-888-397-3742
- TransUnion: transunion.com or 1-800-680-7289

Notify Individuals

If the firm quickly notifies people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused. In deciding who to notify, and how, firms should consider:

- State laws;
- The nature of the compromise;
- The type of information taken;
- The likelihood of misuse; and
- The potential damage if the information is misused.

For example, thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name but also to commit tax identity theft. People who are notified early can take steps to limit the damage.

When notifying individuals, the FTC recommends that the firm:

- Consult with the law enforcement contact about the timing of the notification so it doesn't impede the investigation;
- Designate a point person within the organization for releasing information. Give the contact person the latest information about the breach, the firm's response, and how individuals should respond. Consider using letters (see sample below), websites, and toll-free numbers to communicate with people whose information may have been compromised. The firm can build an extensive public relations campaign into its communications plan, including press releases or other news media notification; and
- Consider offering at least a year of free credit monitoring or other support such as identity theft protection or identity restoration services, particularly if financial information or Social Security numbers were exposed. When such information is exposed, thieves may use it to open new accounts.

Most states have breach notification laws that tell you what information you must, or must not, provide in the firm's breach notice. In general, unless state law says otherwise, you'll want to do the following:

- After consulting with law enforcement to ensure the firm's notice will not impede the investigation, clearly describe what is known about the compromise, including -
    - How it happened,
    - What information was taken,
    - How the thieves have used or may use the information (if known),
    - What actions the firm has taken to remedy the situation,
    - What actions the firm is taking to protect individuals, such as offering free credit monitoring services, and
    - How to reach the relevant contacts in the organization.
- Tell people what steps they can take, given the type of information exposed, and provide relevant contact information. For example, people whose Social Security numbers have been stolen should contact the credit bureaus to ask that fraud alerts or credit freezes be placed on their credit reports and contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. See IdentityTheft.gov/databreach for information on appropriate follow-up steps after a compromise, depending on the type of personal information that was exposed. Consider adding this information as an attachment to the firm's breach notification letter, as done in the model letter below.
- Include current information about how to recover from identity theft. For a list of recovery steps, refer consumers to IdentityTheft.gov.
- Consider providing information about the law enforcement agency working on the case, if the law enforcement agency agrees that providing such information would help. Identity theft victims often can provide important information to law enforcement.

- Encourage people who discover that their information has been misused to file a complaint with the FTC, using IdentityTheft.gov. This information is entered into the Consumer Sentinel Network, a secure, online database.
- Describe how the firm will contact consumers in the future**.** For example, if you'll only contact consumers by mail, then say so. If you won't ever call them about the breach, then let them know. This information may help victims avoid phishing scams tied to the breach, while also helping to protect the company's reputation. Some organizations tell consumers that updates will be posted on their website. This gives consumers a place they can go at any time to see the latest information.

Model Letter

The following letter is a model for notifying people whose names and Social Security numbers have been stolen. When Social Security numbers have been stolen, it's important to advise people to place a free fraud alert on their credit reports. A fraud alert may hinder identity thieves from getting credit with stolen information because it serves as a signal to creditors to contact the consumer before opening new accounts or changing existing accounts.

Also, advise consumers to consider placing a credit freeze on their file. The cost to place and lift a freeze depends on state law. Consider attaching the relevant section from IdentityTheft.gov, based on the type of information exposed in the breach. The optional attachment included in Appendix II is for a data breach involving Social Security numbers. There is similar information about other types of personal information.

[Name of Institution/Logo] _____ _____ Date: [insert date]

NOTICE OF DATA BREACH

Dear [Insert Name]:
We are contacting you about a data breach that has occurred at [insert Company Name].

What Happened?	[Describe how the data breach happened, the date of the breach, and how the stolen information has been misused (if you know)].
What Information Was Involved?	This incident involved your [describe the type of personal information that may have been exposed due to the breach].
What We Are Doing	[Describe how the firm is responding to the data breach, including: what actions the firm has taken to remedy the situation; what steps the firm is taking to protect individuals whose information has been breached; and what services the firm is offering (like credit monitoring or identity theft restoration services).]
What You Can Do	We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud

	alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days. Equifax: equifax.com or 1-800-525-6285 Experian: experian.com or 1-888-397-3742 TransUnion: transunion.com or 1-800-680-7289 Request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report and call [insert contact information for law enforcement if authorized to do so]. Get a copy of the police report; you may need it to clear up the fraudulent debts. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations. You also may want to consider contacting the major credit bureaus at the telephone numbers above to place a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identify thief can open new accounts in your name. The cost to place and lift a freeze depends on state law. Find your state Attorney General's office at naag.org to learn more. We have enclosed a copy of *Identity Theft: A Recovery Plan*, a comprehensive guide from the FTC to help you guard against and deal with identity theft. We've also attached information from IdentityTheft.gov about steps you can take to help protect yourself from identity theft, depending on the type of information exposed.
Other Important Information	[Insert other important information here.]
For More Information	Call [telephone number] or go to [Internet website]. [State how additional information or updates will be shared/or where they will be posted.]

[Insert closing]
Your Name

Summary

- If a breach occurs, preserve customer data and consider notifying consumers, law enforcement, and/or businesses
- Quickly stop additional data loss, secure the firm's systems and fix vulnerabilities that may have caused the breach by:
  - Assembling a team of experts to conduct a comprehensive breach response
  - Considering hiring outside legal counsel with privacy and data security expertise to advise on federal and state laws
  - Securing physical areas potentially related to the breach
- Remove improperly posted information from the Internet
- Talk with the people who discovered the breach and anyone else who may know about it
- Fix the vulnerabilities that caused or may have led to the breach, including:
  - Addressing the firm's service providers
  - Considering the firm's network segmentation
  - Working with forensics experts
- Create a comprehensive plan that reaches all affected audiences
- Notify law enforcement—the local police department, the local office of the FBI or the U.S. Secret Service and, if the breach involved mail theft, the U.S. Postal Inspection Service—other affected businesses, and affected individuals
- If names and Social Security numbers have been stolen, contact the major credit bureaus for additional information or advice
- If a compromise involves a large group of people, advise the credit bureaus if recommending fraud alerts and/or credit freezes
- When notifying individuals:
  - Consult with law enforcement to ensure notification doesn't impede the investigation
  - Designate a point person within the organization for releasing information
  - Consider offering at least a year of free credit monitoring or other appropriate support

Chapter Review

1. Why would a firm that has been the victim of a cyber attack need to consult with local law enforcement when notifying individuals about the breach?

   A. To determine if applicable laws require notification

   B. To alert police about the possibility of identity theft

   C. To ensure notification does not impede the investigation

   D. To avoid liability for the breach

2. Sarah has just learned that her tax preparer's files have been hacked and that her Social Security number has been stolen. What should the tax preparer advise her to do?

   A. Request her Social Security number be changed

   B. Request that a free fraud alert be placed on her credit report

C. Contact the firm's attorney to learn her legal remedies

D. Contact local law enforcement

Glossary

Adware	Adware is a generally-benign type of spyware designed to cause advertisements—often unexpected and unwanted—to pop up when the user is on the Internet.
Computer virus	Computer viruses are software programs that, once on the victim's computer, copy themselves by modifying other computer programs on the computer and inserting their own code in them.
Consumer	A "consumer" is someone who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes; the term does not apply to commercial clients.
Customer	A "customer" is a person who has a continuing relationship with the firm. It is the nature of the relationship—whether or not it is an ***ongoing*** relationship—rather than its ***actual duration*** that defines the firm's customers.
Cybercrime	The term "cybercrime" refers to criminal activities carried out by means of a computer or the Internet.
Data breach	A data breach is an event—either accidental or intentional—that discloses an individual's name and financial information and potentially puts that person at risk.
Denial-of-service attack	A denial-of-service attack is a cybercrime designed to stop users from accessing a host website connected to the Internet.
Direct costs (following data breach)	Direct costs incurred following a data breach are the direct cash outlays to accomplish a remediation activity, such as staffing a help desk.
Financial Privacy Rule	The Privacy of Consumer Financial Information Rule (otherwise known as the Financial Privacy Rule) aims to protect the privacy of their customers by requiring financial institutions, including professional tax preparers, data processors, affiliates, and service providers to give their customers privacy notices that explain the financial institution's information collection and sharing practices.
Glass-Steagall Act	Legislation providing federal insurance for bank depositors and requiring the separation of commercial and investment banking, formally referred to as the Banking Act of 1933.
Gramm-Leach-Bliley (GLB) Act	Legislation passed in 1999 that generally removed the barriers between the banking, securities and insurance industries erected by Glass-Steagall and directed the Federal Trade Commission (FTC) to establish the Financial Privacy Rule and the Safeguards Rule, both of which address tax preparers' vulnerability to cyberattacks.
Indirect costs (following data breach)	Indirect costs are the expenses related to the amount of time, effort and allocation of organizational resources to identify and resolve the data breach.
Information Security Program	The Information Security Program, required under the Safeguards Rule, contains administrative, technical, and physical safeguards appropriate to the business' size and complexity, nature and scope of activities, and sensitivity of customer information it handles.
Malware	The term "malware" is simply a contraction of the words ***malicious software*** and is used to refer generally to various types of harmful or intrusive software secretly installed and intended to act against the interests of the computer user.

Media	The term "media," as used in connection with information security, refers to any method of presenting and/or storing information and includes computer disks, tapes, compact disks, flash drives, audio and video recordings, and paper documents.
Network segmentation	Network segmentation refers to barriers built into a network so that a breach on one server or in one site could not lead to a breach on another server or site.
Opportunity cost (following data breach)	Opportunity cost refers to the loss of current clients and future business resulting from public disclosure of a data breach involving client non-public information.
Opt-out notice	An opt-out notice is a notice required of financial institutions that disclose non-public information (NPI) describing a way for consumers and customers to prohibit many types of NPI disclosure to nonaffiliated third parties before the firm can disclose their NPI.
Phishing	Phishing is a social engineering confidence scam usually designed to manipulate an intended victim into disclosing sensitive personal information or accessing a Website that will download malware to the intended victim's computer.
Privacy notice	An initial and annual notice financial institutions must provide for customers describing the types of information about customers the business collects and to whom it makes the collected information available.
Ransomware	Ransomware is a type of malware that locks or encrypts the digital files contained on a business' computer, thereby prohibiting access to the computer, and enables the cyber criminal to demand a ransom to again give the business access to its files.
Safeguards Rule	Safeguards Rule, required by the GLB, requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure and mandates that financial institutions develop, implement and maintain a written and accessible Information Security Program.
Sarbanes-Oxley Act	Legislation passed in 2002 requiring, in connection with safeguarding customer information, that SEC-reporting companies with a market capitalization in excess of $75 million establish an infrastructure to protect and preserve records and data from destruction, loss, unauthorized alteration or other misuse.
Spyware	Spyware is computer code that, once downloaded, gathers information about the computer user without the user's consent or knowledge and transmits it to a third party.
Trojan horse	"Trojan horse," as used in connection with cybercrime, refers to benign-appearing malware that hides a computer virus and which, once downloaded, causes damage to a victim's computer.

Answers to Review Questions

Chapter 1

Question #1 Feedback

A. Your answer is incorrect. The installation of a computer virus can be the result of a prior scam; however, it is seldom the beginning of cybercrime.

B. Your answer is incorrect. Although a criminal may certainly obtain information through mail theft that subsequently leads to cybercrime, there is as far more prevalent way by which cyber criminals gain a victim's trust and information.

C. Your answer is correct. An estimated 90% - 95% of cybercrime begins with a relatively simple social engineering confidence scam referred to as "phishing."

D. Your answer is incorrect. A denial of service attack may temporarily or permanently immobilize a cyber victim's computer system, that is the result of this social engineering scam.

Question #2 Feedback

A. Your answer is incorrect. Computer viruses are software programs that, once on your computer, copy themselves by modifying other computer programs on the attacked computer and inserting their own code in them. Although they may slow or stop a computer from functioning, they don't accomplish that result by flooding the computer with incoming messages.

B. Your answer is correct. A denial-of-service attack is a cybercrime designed to stop users—you, your employees or your potential customers—from accessing a host website connected to the Internet. The attacked "host" may be a resource website that your firm uses or, alternatively, it may be your *firm's* website that is attacked to keep your potential customers from accessing it. It is normally accomplished by flooding the host victim's computer with incoming messages.

C. Your answer is incorrect. The scam used to place computer malware known as a Trojan horse on a victim's computer often starts with the social engineering known as phishing in an attempt to encourage a computer user to open a harmless appearing attachment to an email. When that occurs, the malicious computer code contained in it begins to accomplish the tasks for which it was programmed, tasks that may include causing the computer to stop.

D. Your answer is incorrect. A tracking cookie is computer code that, once downloaded, gathers information about the computer user—generally without the user's consent or knowledge—and transmits it to a third party. A tracking cookie, although benign, is considered spyware.

Question #3 Feedback

A. Your answer is correct. If an email contains a link to a website, it is a good idea NOT to click on it. However, if you just rest the cursor over the link, you can see the actual URL for the website to which clicking on the link will take you. If the address shown by hovering over the link fails to match the link typed into the message, you can be reasonably certain that it is a phishing attempt.

B. Your answer is incorrect. If the URL link is a way that a cyber criminal is attempting to compromise an intended victim's computer, speaking to the criminal is only putting the computer at greater risk by increasing the chances of a successful phishing attempt.

C. Your answer is incorrect. If an email contains a link to a website, it is a good idea NOT to click on it. By clicking on a bogus link, any computer virus embedded in the website will immediately be transferred to the victim's computer.

D. Your answer is incorrect. Although many links sent to an intended victim's email account are persuasive, a method is available to see if it has a high potential for being a phishing attempt.

Chapter 2

Question #1 Feedback

A. Your answer is incorrect. Although certain clients of a professional tax preparer that shares no non-public information need not be sent a privacy notice, such a notice must be provided to other clients.

B. Your answer is incorrect. A tax preparer is required to provide a privacy notice to a consumer only if it shares certain non-public information. However, a tax preparer that does not engage in such sharing does not.

C. Your answer is incorrect. A privacy notice need not be furnished to all of a tax preparer's clients if it does not share non-public information.

D. Your answer is correct. Whether or not the firm shares customer non-public personal information (NPI), the firm must give all its customers a privacy notice. The firm is required to provide an initial notice and an annual notice.

Question #2 Feedback

A. Your answer is correct. If a firm shares NPI with nonaffiliated third parties outside of specified exceptions, the firm must give its customers an "opt-out" notice, a reasonable way to opt out and a reasonable amount of time to opt out before the firm discloses the NPI.

B. Your answer is incorrect. The payment of a stipend does not meet the FTC requirement when a firm shares its customers' NPI with a nonaffiliated third party.

C. Your answer is incorrect. Even though a firm explains its reasons for sharing a customer's NPI with a nonaffiliated third party, such an explanation will not meet the FTC's requirement in such a case.

D. Your answer is incorrect. If the firm is required under the FTC rules to provide a privacy notice to its consumers because of its NPI-sharing policies, the firm may choose to give them a short-form notice explaining that the firm's full privacy notice is available on request and provide additional information. Such a short-form notice will not enable the firm to meet its FTC requirement, however.

Chapter 3

Question #1 Feedback

A. Your answer is incorrect. Unfortunately, your answer is too low. The cost per compromised record in a data breach, according to the 2017 IBM study, exceeded $137.

B. Your answer is correct. According to a 2017 study commissioned by IBM and undertaken by the Ponemon Institute, LLC on the cost of a data breach, the average cost to a financial services organization—a category that includes professional tax preparers—for each compromised record was $245.

C. Your answer is incorrect. Although a tax preparer's cost per compromised record could be as high as $376, depending on its remediation activities following a data breach, the average found in the 2017 IBM study was lower.

D. Your answer is incorrect. While any firm's cost per compromised record could be as high as $483, depending on its remediation activities following a data breach, the average found in the 2017 IBM study was lower.

Question #2 Feedback

A. Your answer is incorrect. While the study's claim that the probability of a data breach occurring in the next 24 months is an estimate that may turn out to be too high or too low, it exceeds 9.4%.

B. Your answer is incorrect. Although the statement that the probability of a data breach occurring in the next 24 months is an estimate, it is greater than 17.3%.

C. Your answer is correct. According to the 2017 IBM-Ponemon study, the probability of a material data breach occurring at any organization over the next 24-month period is estimated to be 26.8%

D. Your answer is incorrect. Even though the likelihood of a data breach may reach or exceed 37.9% in the next 24-month period depending on the increased sophistication of cyber criminals and the failure to take precautions, the 2017 IBM study estimate was lower.

Chapter 4

Question #1 Feedback

A. Your answer is incorrect. Ensuring that employees having access to taxpayer information sign a nondisclosure agreement *is* a recommendation designed to reduce the likelihood of a cyberattack by current and/or former employees.

B. Your answer is incorrect. By revoking the access to taxpayer information that had been given to terminating employees and employees who no longer require such access can be expected to reduce the probability of a cyberattack by current or former employees.

C. Your answer is incorrect. Retrieving all property that permits a terminating employee to access taxpayer information is a recommended precaution for all such employees regardless of the reason for the employee's termination. When an employee is terminated involuntarily by the firm, ensuring the inability to access taxpayer information takes on even greater importance.

D. Your answer is correct. While immediately escorting a terminating employee from the firm's premises may be appropriate in unusual situations, it is not a recommended procedures. However, to reduce the probability of a cyberattack by a current or former employee, the firm's Information Security Plan should require that:
   - Nondisclosure agreements be signed by any personnel who will have access to confidential taxpayer or firm proprietary information;
   - Access to taxpayer information (e.g., login IDs and passwords) be immediately stopped for those employees who are terminated or who no longer need access; and
   - An exit interview be conducted with each terminated employee during which all property that allows access to taxpayer information (e.g., laptops, media, keys, identification cards and building passes) be returned to the firm.

Question #2 Feedback

A. Your answer is incorrect. While employee negligence can lead to costly data breaches, such negligence is not the cause of the costliest such breaches largely because it is unintentional and not motivated by the intent to steal information.

B. Your answer is correct. Although taxpayer and firm data certainly may be compromised or lost as a result of employees' unintentional failure to take appropriate precautions, the more sinister and costly cause is a cyberattack mounted by someone intent on stealing company and taxpayer information.

C. Your answer is incorrect. Employee ignorance may be a cause of data loss, but its correction is fairly simple and inexpensive. It is not the costliest source of data breaches.

D. Your answer is incorrect. Glitches in business process may certainly occur and cause a data breach, particularly if the process is new and untried. However, such a data breach, although possibly causing firm embarrassment is seldom considered the costliest cause.

Chapter 5

Question #1 Feedback

A. Your answer is incorrect. Although firm executives would normally be granted access to taxpayer information, the individual's status within the organization should not normally be a definitive criterion with respect to such access.

B. Your answer is incorrect. The criterion applied to those to whom access to taxpayer information is granted should not be the full-time status of the employee.

C. Your answer is incorrect. Even though firm CPAs are likely to be granted access to taxpayer information, the decision to grant such access should not depend on whether or not the employee possesses professional credentials.

D. Your answer is correct. In order to reduce the likelihood of data breach, firms should limit access to customer information only to those employees who have a business reason to see it.

Question #2 Feedback

A. Your answer is correct. The security of stored taxpayer information is enhanced if, where possible, sensitive customer data is NOT stored on a computer with an Internet connection.

B. Your answer is incorrect. Although using an easily-remembered password may help you keep from forgetting it, using an easily-remembered password makes it easier for a cyber criminal to hack into your account.

C. Your answer is incorrect. Storage of customer information on line makes it easier for a cyber criminal to access the information. Normally, customer records should be maintained offline.

D. Your answer is incorrect. If sending customer information across the Internet, the material should always be encrypted.

Chapter 6

Question #1 Feedback

A. Your answer is incorrect. Federal law and FTC regulations require notification. If there is uncertainty concerning notification of consumers, such questions should be directed to competent attorneys.

B. Your answer is incorrect. While alerting law enforcement that a data breach may result in identity theft would be important, that is not the concern with respect to notifying individuals about the breach.

C. Your answer is correct. When notifying individuals concerning a data breach, the FTC recommends that the firm consult with the law enforcement contact about the timing of the notification so it doesn't impede the investigation.

D. Your answer is incorrect. The firm's liability for the breach and any damages that may result are not determined based on its notification of local law enforcement personnel.

Question #2 Feedback

A. Your answer is incorrect. In most cases, an assigned Social Security number cannot be changed and is retired upon your death. However, changing a Social Security number may be approved for individuals placed in a witness protection program. The circumstances for changing an existing Social Security number must be serious, extenuating and provable.

B. Your answer is correct. When Social Security numbers have been stolen, it's important to advise people to place a free fraud alert on their credit reports. A fraud alert may hinder identity thieves from getting credit with stolen information because it serves as a signal to creditors to contact the consumer before opening new accounts or changing existing accounts.

C. Your answer is incorrect. If a customer whose Social Security number had been stolen from the records of a professional tax preparer wanted to determine the legal remedies available to her, she would consult an attorney not associated with the preparer.

D. Your answer is incorrect. Law enforcement notification would already have been made by the firm. However, she may wish to also make such notification.

Index

Appendix I

Examples of Controls Contained in Rules of Behavior

- Delineate responsibilities, expected use of system, and behavior of all users.
- Describe appropriate limits on interconnections.
- Define service provisions and restoration priorities.
- Describe consequences of behavior not consistent with rules.
- Covers the following topics:
  - Work at home
  - Dial-in access
  - Connection to the Internet
  - Use of copyrighted work
  - Unofficial use of government equipment
  - Assignment and limitations of system privileges and individual accountability
  - Password usage
  - Searching databases and divulging information.

Source: National Institute of Standards and Technology "Guide for Developing Security Plans for Federal Information Systems," NIST Special Publication 800-18.

Return to text

Appendix II

OPTIONAL ATTACHMENT- data breach involving Social Security numbers*

FEDERAL TRADE COMMISSION
IdentityTheft.gov

What information was lost or exposed?

Social Security number

- If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
- Get your free credit reports from annualcreditreport.com. Check for any accounts or charges you don't recognize.
- Consider placing a credit freeze. A credit freeze makes it harder for someone to open a new account in your name.
    - If you place a freeze, be ready to take a few extra steps the next time you apply for a new credit card or cell phone —or any service that requires a credit check.
    - If you decide not to place a credit freeze, at least consider placing a fraud alert.
- Try to file your taxes early — before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.
- Don't believe anyone who calls and says you'll be arrested unless you pay for taxes or debt — even if they have part or all of your Social Security number, or they say they're from the IRS.
- Continue to check your credit reports at annualcreditreport.com. You can order a free report from each of the three credit reporting companies once a year.

*Consider attaching the relevant section from IdentityTheft.gov, based on the type of information exposed in the breach. This is for a data breach involving Social Security numbers. There is similar information about other types of personal information.

Return to text

Final Exam

Keeping Taxpayer Data Secure

The following exam is attached only for your convenience. To access the official exam for this self-study course, please log into your account online and take the Final Exam from the course details page. A passing score of 70 percent or better will receive course credit and a Certificate of Completion.

1. How could a computer virus allow a third party to access a host computer's passwords?
   A. By disclosing computer keystrokes
   B. By denying access to the computer until the operator voluntarily discloses passwords
   C. By using adware
   D. By spoofing
2. The type of malicious code that encrypts a computer's digital files unless the user pays a fee is known as:
   A. spyware
   B. a Trojan horse
   C. ransomware
   D. phishing
3. _____ refers to deceptive manipulation of a computer user known as "social engineering."
   A. A Trojan horse
   B. Spyware
   C. Adware
   D. Phishing
4. The _____ requires tax preparers to develop, implement and maintain an Information Security Program.
   A. Privacy Rule
   B. Safeguards Rule
   C. Glass-Steagall Act
   D. Tax Cuts and Jobs Act
5. Whether or not a tax preparer firm shares non-public personal information (NPI), the firm must give all its _____ a privacy notice.
   A. service providers
   B. consumers
   C. customers
   D. nonaffiliated third parties
6. The costs to a victimized firm of a data breach generally include all of the following EXCEPT
   A. direct cash outlays to provide additional staffing, etc.
   B. expenses associated with the use of firm resources to identify and resolve the breach

C. opportunity costs

D. penalty costs

7. What is the average cost of a data breach in a small to medium size business?

   A. $25,000

   B. $52,000

   C. $117,000

   D. $211,000

8. Which of the following tax preparer firm initiatives has been shown to most significantly reduce the loss of existing customers following a data breach?

   A. Programs designed to enhance customer trust

   B. Charging deeply discounted fees

   C. Implementing a program of increased customer communications

   D. Charging customer fees based on the refund obtained

9. When writing the physical facility part of its Information Security Plan, which of the following must the firm consider?

   I. Each PC and computer laptop used for accessing or storing taxpayer information

   II. The central computer room

   III. Delivery and removal of taxpayer information

   A. I & II only

   B. I & III only

   C. II & III only

   D. I, II and III

10. Which of the following must a firm address when writing the Personnel Security portion of its Information Security Plan?

   I. Data breach resulting from human error

   II. Intentional unauthorized access

   A. I only

   B. II only

   C. Both I & II

   D. Neither I nor II

11. The FTC suggests requiring the lock-out of computer system users after _____ consecutive invalid access attempts.

   A. 3

   B. 4

   C. 7

   D. 9

12. Which of the following should be done when electronically transmitting sensitive financial data?

   I. Use a Secure Sockets Layer

   II. Encrypt the data

A. I only

B. II only

C. Both I & II

D. Neither I nor II

13. An FTC best practice to help ensure the security of customer information by a firm that uses a broadband Internet connection calls for

A. maintaining up-to-date firewalls

B. limiting use of customer files

C. avoiding use of the firm's service providers

D. encrypting stored customer data

14. What steps should a tax preparer take to preserve customer data in the event of a data breach?

I. Secure any information that has been or may have been compromised

II. Preserve and review files or programs that may reveal how the breach occurred

III. Use security professionals to help assess the breach

A. I & II only

B. I & III only

C. II & III only

D. I, II and III

15. What organization should be notified in the event of a data breach if the local police aren't familiar with investigating information compromises?

A. The FBI or U.S. Secret Service

B. State police

C. U.S. Postal Inspection Service

D. The Federal Trade Commission