LAWDESK

INFORMATION SECURITY PROGRAM

TRAINING

Information Security Program Training

Background

Identity theft and information security breaches continue to affect millions of people each year. Just look at some of these statistics:

- Approximately 15 million Americans have their identities used fraudulently each year -- that's an estimated 7% of all adults
- Financial losses total upwards of $50 billion
- Each instance of identity theft results in approximately $3,500 in losses
- Close to 100 million Americans have their personal identifying information placed at risk of theft each year due to security breaches

These are alarming statistics. So, what can you do to help reduce these numbers? Take information security seriously and implement robust information security programs to protect information.

- Protection of information assets is necessary to:
    - Establish and maintain your customers' trust;
    - Comply with the law; and
    - Protect the Company Lending's reputation.

Basics

So, what exactly is **information security**? Information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations.

Information security has three main objectives: (1) **confidentiality**, (2) **integrity** and (3) **availability**. These objectives are commonly referred to as the CIA triad.

- **Confidentiality** - Protecting information against unauthorized access or use
- **Integrity** - Preserving information so that it is not accidently or intentionally altered
- **Availability** - Ensuring authorized users have prompt access to information

It is important to protect information because the Company Lending's profitability can be negatively affected if information becomes known to unauthorized parties, is altered without proper authorization, or is not available when it is needed.

An **Information Security Program** must:

- Ensure security and confidentiality;
- Protect against anticipated threats, including unauthorized access or use; and
- Ensure proper disposal.

The Program must have strong **board and senior management support**, integration of security activities and controls throughout the Company Lending's processes, and provide for clear accountability for carrying out security responsibilities. Additionally, the Company must update its Program to account for changes in controls, threats, technologies, and business conditions.

So, you may be thinking, information security doesn't apply to me because the Company uses technology, such as firewalls, to prevent security breaches and our IT department is responsible for that. Well, that could not be further from the truth. Information security does apply to YOU!

What do we mean by layers of security? **Layered security**, often referred to as defense in depth, is security applied in overlapping layers that provides three elements needed to secure assets. The three elements are known as: (1) **prevention**, (2) **detection**, and (3) **response**.

Let's take a look at an example that illustrates the three elements of **layered security**.

Example: Cash, an important asset of a financial institution, is stored in a vault. Access to the vault requires passing through layers of security. Those layers of security include human guards and locked doors with special access codes. Additionally, the vault may be monitored by closed-circuit televisions, motion sensors, and alarm systems that can quickly detect unusual activity. The sound of an alarm may trigger the doors to automatically lock and the police to be notified.

- **Preventative Controls**: In this example, human guards and locked doors with special access codes are examples of preventative controls.

- **Detective Controls**: The detective controls consist of monitoring the vault by closed-circuit televisions, motion sensors and alarm systems.

- **Response Controls**: Finally, the response controls consist of automatically locking doors and police notification.

It is important to remember that you are one of the Company Lending's most important layers of security. How well you prevent, detect and respond to security threats directly impacts the effectiveness of the Company Lending's Information Security Program.

Security Threats

In order for you to be an effective layer of security, you must become familiar with common security threats. Some of the top threats affecting institutions include:

- Malware
- Mobile Devices
- Social Networks
- Social Engineering
- ACH Fraud
- Insiders
- First-Party Fraud
- Skimming

Each of these threats will be described more fully.

(1) Malware

Malware, short for malicious software, is designed to access a computer without the knowledge or permission of the user. Malware may be used to gather or destroy information. **Examples** of malware include: viruses, worms, Trojan horses, spyware, keyloggers and rootkits.

(2) Mobile Devices

Mobile devices, such as smart phones, laptops and USB drives, are becoming more and more of a common security threat. One of the major threats associated with these devices, especially laptops, is **theft**. Each year thousands of laptops are stolen and sensitive data is compromised. Mobile devices are increasingly being used for financial services. However, security associated with these devices has proven to be more challenging than traditional online banking. These devices are particularly vulnerable to malware that can steal financial data.

(3) Social Networks

Social networking refers to an online service that allows individuals and organizations to interact with each other. Users generate the content and post and edit conversations, pictures and media. Some of the most popular social **media sites include** Facebook, Linkedin, Twitter and YouTube. As institutions embrace social networking sites, so too are information thieves. One way information thieves target these sites is by creating fake sites to try to trick people into giving up personal information.

The risks associated with social networking sites do not stop with inadvertently disclosed information. Indeed, institution employees often access these social networking sites and intentionally or unintentionally expose sensitive information. This is why it is important to follow the Company's policies on when and how to use social networks.

(4) Social Engineering

Gaining information by tricking an individual into releasing information is often referred to as social engineering. Here are some common social engineering techniques:

- **Face-to-Face** - Approaching someone in person to request information while posing as someone in a position of authority, such as a manager or information security staff.
- **Phishing** - Sending fake emails, disguised as messages from legitimate sources, to gain access to sensitive information.
- **Pharming** - Directing an individual to unauthorized websites that request the individual to disclose sensitive information.
- **Dumpster Diving** - Digging through trash (e.g., trash cans or shred-bins) in order to gather information.
- **Phone Calls** - Posing as a customer or someone of authority (e.g., law enforcement or information security personnel) over the phone in order to obtain information.
- **Shoulder Surfing** - Gathering information by surreptitiously visually observing or photographing information entered at locations from which confidential or other sensitive information is disclosed, such as at ATM machines or computer workstations.
- **Eavesdropping** - Illicitly listening in on employee phone calls, office conversations or meetings to gain information.
- **Man-in-the-Middle** - An attack in which a fraudster is able to read, insert into and modify messages between two parties without either party knowing that the link between them has been compromised.
- **Man-in-the-Browser** - This technique is related to man-in-the-middle. It is a Trojan horse that infects a web browser and has the ability to insert or modify content or transactions, without the user or the host's knowledge.

(5) ACH Fraud

Automated Clearing House ("ACH") fraud is an unauthorized ACH funds transfer that occurs in an account. Unfortunately, ACH fraud is relatively easy to execute. All that is needed is an account and a routing number. In its simplest form, the fraudster uses an account number and routing number to initiate payments for purchases or pay debt. This type of fraud can occur over the phone or though Internet transactions.

More sophisticated ACH fraud involves techniques such as Man-In-the-Middle ("MIM") or Man-In-the-Browser ("MIB"). In a MIM/MIB attack, the fraudster inserts himself between the customer and the institution and hijacks the online session. In one scenario, the fraudster is able to intercept the authentication credentials submitted by the customer and log into the customer's account. In another scenario, the fraudster does not intercept the credentials, but modifies the transaction content or inserts additional transactions not authorized by the customer which, in most cases, are fund transfers by the fraudster.

The fraudsters conceal their actions by directing the customer to a fraudulent website that is a mirror image of the institution's website or by sending the customer a message claiming that the institution's website is unavailable and to try again later.

(6) Insiders

Malicious attacks or hacks are often launched inside an institution by a desperate or disgruntled employee. The following are actual accounts of insider threats:

- A former employee allegedly planted a logic bomb at a mortgage finance company. Had it not been discovered, the logic bomb would have shut down the company for at least a week and destroyed all servers, causing millions of dollars in lost productivity and other damages.

- Law enforcement charged a former bank employee with grand larceny, identity theft, and money laundering after he stole the identities of more than 150 bank employees and used them to steal over $1.1 million from charities, non-profit organizations and other entities.

- A court sentenced a former bank employee to two years in prison and ordered her to pay restitution for bank fraud and aggravated identity theft, which stemmed from her role in a scheme that defrauded her employer of more than $300,000.

Careless and untrained employees also pose serious security threats to the Company Lending. Accidental disclosure of confidential information occurs more frequently than deliberate incidents. For example, an employee's manager asked him to send a statement to a customer. The employee sent the information to the wrong email account and also attached a file containing the confidential information of 1,325 other customers including their names, addresses, and social security numbers.

(7) First-Party Fraud

First-party fraud, also known as "advances fraud," "application fraud," "friendly fraud" and "sleeper fraud," occurs when individuals provide false or deceptive information about themselves in order to obtain a financial product or service. For example, customers may use false identification or misrepresent other information, such as a Social Security number.

(8) Skimming

Skimming is the theft of card information used in an otherwise legitimate transaction. Typically, the fraudster obtains the victim's card number by using a card reader to swipe and store hundreds of card numbers.

Best Practices

Do…

- Take responsibility for securing information
- Report known or suspected security issues
- Recognize confidential information and ensure it is protected
- Follow your institution's Internet usage policy
- Use secure forms of email when transmitting sensitive information
- Use strong and complex passwords
- Inform your IT department if you need additional software instead of installing it on your own
- Use mobile devices with security features
- Lock your computer and keep your desk clear of confidential information while you are away from your desk
- Dispose of confidential information properly
- Follow all laws, regulations and security policies

Don't…

- Assume security is someone else's job
- Fail to report security issues - without reporting, security issues cannot be resolved and future incidents cannot be prevented
- Share confidential information with any unauthorized person, discuss it in public places or store it in unsecured mobile devices
- Use workplace resources to access inappropriate materials
- Send unsecured email when transmitting sensitive information
- Use passwords that are simple and easily guessed
- Download or install unapproved software from the Internet
- Place confidential information on unsecured laptops, USB drives or smart phones
- Forget to use a password protected screensaver so that no one can access your computer while you are away from your desk
- Keep information indefinitely or disregard record retention rules
- Bend, break or look the other way when it comes to security, even if you are busy or it is an inconvenience

Conversations

Be diligent when disclosing confidential information. Avoid discussing any information in a casual or non-businesslike way, both inside and outside of the workplace.

> **Example 1**: You learn about the spending habits of a local, prominent businessman when monitoring his account. Even though it may be tempting to tell your friends about the transactions, you must not. It is confidential information that you must not share with anyone else.

Example 2: Your spouse is a banker who wants to attract new clients. She asks you for the names of customers who have recently obtained accounts. Even though her request seems harmless, you must not provide this information.

Desks

Keep your office, desk, or workspace, clear of confidential information while you are away. This includes:

- Clearing off your desktop when you are not in your work area;
- Keeping information stored in file folders rather than in piles of loose papers;
- Locking rooms, drawers and file cabinets where information is stored; and
- Using password-activated screensavers that require a log-in after a period of inactivity.

Passwords

Your password is a unique set of characters that is used to verify your identity prior to accessing information. Your password should be strong and complex. That is, it contains **8 or more characters** with upper and lower case letters, numbers and special characters.

Passwords should be difficult to guess. Using the passphrase method to create your password is a good way to remember it.

- Think of something memorable or familiar, like a friend's spouse's birth date.
- Write a sentence based on this thought. For example, "John was born in 1995."
- Use the first letter of each word, and keep the case of the first letter as it appears in the sentence. Use the numbers as replacements for words whenever possible (e.g., 2 for "two" or "to" and 4 for "four" or "for") and include punctuation, numbers and symbols. Using the sentence in step 3 as an example, the password would be "Jwbi1995."

Protecting your password is an important security responsibility. Here are some additional ways to protect your password:

- Do not enter a password on help desk support request forms
- Do not write passwords down and store them insecurely
- Do not send passwords in an email message
- Never disclose a password over the phone
- Do not allow co-workers to use your password while you are on vacation
- Do not share passwords with friends or family
- Do not reveal your password to your manager, even if he or she asks for it
- Change your password immediately if you think that it has been compromised
- Change your password periodically (e.g., once every 30 days)

Email

The misuse of email can create security exposures. Some common guidelines for using email include:

- Do not provide usernames and passwords via email
- Do not open emails from senders that you do not recognize or open attachments from people that you do not know or trust

- Do not open executable or scripting attachments (e.g., attachments that end in .exe, .vbs., .bat, .cmd)
- Do not transmit confidential information unless it is encrypted
- Use caution when opening or saving compressed files (e.g., those with the .zip extension)

Voice Mail and Fax

Using voice mail, fax machines, copy machines, and participating on conference calls are all part of our work day. You must maintain the confidentiality of the information discussed, transmitted or duplicated.

- Always use a password to protect your voice mail
- Do not share your voice mail password with anyone
- If you are faxing information, call ahead to ensure that the recipient is available to receive the information
- If you are expecting an incoming fax, ensure that you promptly remove it from the fax machine

Internet

The Company should have an Internet usage policy, which includes prohibiting:

- Personal use of the Internet
- Use of the Internet to transmit or view obscene, sexually explicit, threatening or illegal content
- Usage that places an excessive strain on systems, network or personnel resources

Examples of inappropriate use are:

- Using Internet gambling sites;
- Intentionally transmitting or viewing pornographic or racist material;
- Downloading files that infringe on copyrights, such as movie or music files; and
- Accessing or attempting to access confidential information or system resources without proper authorization.

Mobile Devices

Mobile devices, such as laptops, USB drives and smart phones, must be properly managed and maintained. Here are some best practices:

- Be aware of the location of your mobile device at all times
- Never leave your mobile device visible in a vehicle – take it with you whenever possible
- Carry your laptop in an inconspicuous bag that does not look like a laptop bag
- Do not store confidential information on a mobile device
- If you must store confidential information on a mobile device, use encryption
- Always use a strong password on a mobile device

Social Engineering

Social engineering relies on deception and the vulnerability of its victims. A sophisticated con artist can fool even experienced personnel.

To protect you and the Company from social engineering, consider these best practices:

- Do not give out information about employees, practices, or strategies to anyone you do not know or believe does not have a need to know
- Refer requests for information to designated individuals or a manager
- Do not assume that just because someone knows your institution's internal "lingo" that they are an employee
- Obtain a customer's written permission before disclosing confidential information
- Never provide a caller with your password
- Never respond to unsolicited email messages that request personal information
- If you suspect someone of social engineering, promptly report the activity to a manager or security officer

Physical Security

Employees play an important role in ensuring Companyis a safe place to work. Malicious individuals may try to obtain unauthorized access to offices to steal equipment, confidential information, and other valuable assets.

Best practices for physical security:

- Ensure that employees have proper identification
- Do not allow unauthorized individuals into restricted areas
- Prevent unauthorized visitors from tailgating or piggybacking
- Politely ask anyone suspicious: "May I help you?"
- Do not prop secured doors open
- Do not leave anything of value exposed in your office or workspace
- Lock all confidential documents in desk drawers/file cabinets when not in use
- Report suspicious individuals

Disposal of Information

You must discard confidential information according to regulatory guidelines. The guidelines include best practices for handling paper records and provide suggestions for the unique disposal problems posed by computer-based records.

Examples:

- Separate confidential material from regular garbage to keep "dumpster divers" from getting it.
- Shred paper records before discarding or recycling them.
- Compact discs and computer hard drives should be physically destroyed to ensure that no residual data remains on them. Note- Simply deleting electronic files from a computer does not comply because deleted files can be recovered.
- Keep a log of how you disposed of sensitive information, especially information on computer-based media.

Responding to Security Breaches

It is essential that you report any potential security incident, so that it can be investigated. The Company may be required to notify customers whose information has been accessed without authorization or misused. When you suspect unauthorized access, or use of information, you must:

- Notify your supervisor immediately
- Identify which systems and types of information are affected

- If warranted, gather information so a Suspicious Activity Report ("SAR") can be filed
- Notify law enforcement if ongoing criminal violations require immediate attention
- Monitor, freeze or close affected accounts to prevent further unauthorized access
- Preserve all records and evidence of the incident
- Follow the Company's notification procedures

Remember, incidents can originate from outside the Company Lending, such as network attackers, attempts to steal information, or threats to the Company or its employees. They may also originate from inside the Company, such as from a disgruntled worker. Either has the potential to cause serious harm and should be taken seriously.

Noncompliance Consequences

Failing to properly secure information can negatively affect the Company's ability to do business. Consequences can include:

- Disciplinary action against you and your institution
- Criminal charges
- Negative publicity
- Regulatory enforcement actions
- Loss of business opportunities if others refuse to deal with your institution

You are the first line of defense against information thieves. Following the Company's Information Security Procedures helps deter the unauthorized use of information.