Course Content

This content was written for an online course about cybersecurity and personal safety in real estate. The course contained 12 chapters, 15 quiz questions per chapter, and one learning activity per chapter.

Chapter 5
Data Security Program

Overview
Information security is a vital component of an effective cybersecurity strategy because it aims to maintain the availability, confidentiality, and integrity of data. Real estate professionals and businesses should develop and maintain comprehensive and up-to-date data security programs to (a) ensure safe transmittal, access, and storage of personal information; (b) comply with state and federal laws; and (d) reduce the business, financial, and legal risks associated with data breaches. This chapter discusses elements of a data security program.

By the end of this chapter, you will be able to:

• list and explain key principles for creating a data security program;
• use data security principles to develop a data security program; and
• develop a privacy policy.
Elements of a Data Security Program

In its *Data Security and Privacy Toolkit*, the National Association of REALTORS® stated the following about the significance of data security for real estate businesses and professionals:

"Trust is at the heart of the real estate business. In this digital economy, trust has taken on new dimensions that impact how real estate professionals collect, share, and, most important, protect the information they use in their businesses."¹

The toolkit aims to educate real estate agents, associations, brokers, and multiple listing services about the need for data privacy and security. It incorporates the Federal Trade Commission's data security principles—take stock, scale down, lock it, pitch it, and plan ahead—to provide a guide for implementing a well-defined data security program.

Take Stock

Businesses should perform an information inventory to answer four overarching questions:

- What types of information do we maintain and why do we keep it?
- Who maintains and has access to this information?
- How do we collect this information?
- Can consumers and users opt-out of our data collection program?

The more thorough the inventory, the better prepared a business is to develop an effective data security program. To track the type and volume of information collected, businesses should talk to personnel in its accounting, human resources, and information technology departments; vendors; and independent contractors. They should also take inventory of all equipment where data is stored including computers, disks, flash drives, home computers, laptops, and mobile devices.

Information Inventory

Answers to the following questions can help businesses complete a thorough information inventory. Examples of possible answers are listed below each question.

- Who sends our company personal information?
  - Banks or other financial institutions
  - Brokerages
  - Call centers
  - Consumers
  - Contractors
  - Credit card companies
  - Employees
  - Independent contractors

• How does our company receive personal information?
  o Cash registers
  o Emails
  o Interviews
  o Mail
  o Websites

• Where do we store data received at each entry point?
  o Branch offices
  o Central computer database
  o Disks
  o Employees/licensees' home offices
  o File cabinets
  o Individual laptops
  o Mobile devices

• Who has or could gain access to the information?
  o Consumers
  o Independent contractors
  o Members of the public
  o Specific licensees/employees
  o Vendors

• What kind of information do we collect at each entry point?
  o Access codes, passwords, and security codes for financial accounts
  o Biometric data
  o Checking account information
  o Credit card or debit card numbers
  o Credit histories
  o Driver's license numbers
  o Email addresses
  o Financial information (e.g., balance, history, transaction history)
  o Geo-location information
  o Government-issued identification numbers
  o Health insurance information
  o Medical information
  o Mortgage applications
  o Passport numbers
  o Postal addresses
  o Preference profiles (e.g., interest, preferences associated with specific computers, devices, or people)
  o Race/ethnicity
  o Real estate license numbers
  o Religious beliefs
  o Sexual orientation
  o Social security numbers
  o Tax IDs
  o Telephone/fax numbers
  o Persistent identifiers (e.g., customer numbers, IP addresses, user aliases, etc.)
Scale Down

After taking stock of the type of information collected and the reasons for collecting it, businesses should determine whether they need to continue gathering and retaining this type of information. NAR states the following regarding data collection and retention:

"If your association or brokerage does not have a legitimate business need for the personally identifying information, then don’t collect it. If there is a legitimate business need for the information, then keep it only as long as it’s necessary. Once that business need is over, then properly dispose of it."^2

If businesses must keep information for compliance purposes, they should develop a document retention policy that defines the type of data to retain, how it should be secured, the amount of time to retain it, and the method for disposing of it.

Real estate associations and brokerages that collect credit card information, should consider these recommendations for maintaining data security.

- Print only abbreviated credit or debit card numbers on consumer receipts and do not include expiration dates.
- Do not retain credit card account numbers or expiration dates unless necessary.
- Check the default settings on the software that processes transactions to make sure they are not preset to permanently retain unnecessary information.

Lock It

Once a business has performed an information inventory to determine the type of information it collects, how and why it collects this information, and what information it must continue to collect, it can develop a data protection strategy. The Federal Trade Commission recommends encompassing four primary elements in a data protection plan: physical security, electronic security, employee training, and security practices of service providers and contractors. The following checklists provide recommendations for securing personal information.

General Practices

- Physical Security
  - Store files and documents that contain personally identifiable information in locked file cabinets or storage rooms.
  - Only allow employees with legitimate business needs to access information (located both in-house and offsite).
  - Require employees to store file folders in locked cabinets, log off their computers, and lock office doors at the end of the workday.

- Electronic Security

---

o Determine which computers or servers are used to store personally identifiable information.

o Identify all connections to computers and servers with personally identifiable information—such as computers at branch offices, electronic cash registers, online data storage, service providers' computers, and wireless devices.

o Assess each connection's vulnerability to known and foreseeable attacks.

o Refrain from storing personally identifiable information on computers with internet connections unless it is vital for conducting business.

o Encrypt sensitive data sent to third parties over public networks.

o Routinely run current antisyprware and antivirus software on servers and computers in the network.

o Use a secure connection such as Secure Socket Layer (SSL) to transmit sensitive financial data including credit card information.

o Pay close attention to the security of web applications (i.e., software used to provide information to website visitors and collect information from them).

o Require the use of a biometric like a smart card, thumbprint, or token as well as a password to gain access to computers that contain personal information.

Password Management
  • Manage passwords by requiring personnel to create strong passwords (e.g., long passwords with a mix of characters, letters, and numbers).
  
  • Prohibit posting and sharing of passwords.
  
  • Apply password-activated screen savers that lock computers after a certain period of inactivity.
  
  • Educate employees about social engineering. For example, alert employees to the possibility that identity thieves may call them and pose as IT staff members to trick them into providing their passwords. Calls like this are fraudulent because no one should ask for their passwords.
  
  • After installation of new software, immediately replace default passwords with stronger, more secure ones.

Laptop Security
  • Determine if it is necessary to store personal information on laptops and completely remove unnecessary information.
  
  • Encrypt personal information stored on laptops and configure it so users cannot change security settings or download software without authorization from an IT specialist.
  
  • Train employees to remain just as mindful of security while conducting business in the field as they are when working in the office.

Firewalls
  • Use firewalls to protect computers from hackers while on the internet. An appropriately configured firewall makes it more difficult for hackers to locate computers and access files and programs.
• Set access controls to ensure that only reliable employees with valid business needs have access to specific areas of the network.

**Wireless and Remote Access**
• Determine whether employees use wireless devices to transmit personal information or connect to business networks.
• If employees or service providers are given remote access to business networks, consider using encryption to better safeguard information.

**Detecting Breaches**
• Maintain central log files of security-related information to track network activity and identify and respond to cyber-attacks.
• Use an intrusion detection system to identify network breaches as they occur.
• Monitor incoming traffic for signs of hacking.
• Monitor outgoing traffic to identify signs of data breaches.

**Employee Training**
• Conduct background checks and check the references of new hires who will have access to personal information.
• Ensure that employees and independent contractors understand that adhering to data security policies and practices is a vital part of their duties.
• Require employees to notify the appropriate person immediately upon discovering a potential breach of security such as a virus or a lost or stolen laptop.
• Keep an accurate list of employees with access to personal information.
• Develop a procedure to terminate former employees’ access to personal information.
• Establish disciplinary measures for employees who violate security policies.

**Security Practices of Contractors and Service Providers**
• Before outsourcing business functions such as cloud computing, customer call center operations, payroll processing, and web hosting, review service providers’ and contractors’ data security practices to determine if their standards align with company standards.
• Require service providers and contractors to provide notification of security incidents even if no data was compromised.
• Require contractors and service providers to comply with applicable state and federal laws regarding data security and privacy.

**Pitch It**
According to the Federal Trade Commission and laws in many states, appropriate disposal of personal information is a vital part of a data security program. Developing and implementing a document retention policy can help businesses stop unauthorized access to personal information. Typically, proper disposal of personal information involves rendering it unreadable and ensuring that no one can reconstruct it. The Federal Trade Commission suggests burning, pulverizing, or
shredding paper records and using wipe utility programs or other appropriate means to destroy electronic documents.

NAR's process for creating a document retention program includes the following actions:

- Take stock to determine the types and sources of information.
- Identify and document current information retention policies.
- Assess existing policies to determine if changes are necessary.
- Create a comprehensive policy that includes the following information:
  - Length of document retention
  - The policy's purpose, effective date, and last review date
  - The persons responsible for managing the policy
  - The process for preserving records for litigation or anticipated litigation
- Conduct a legal assessment of the document retention policy to ensure legality and compliance with laws and regulations.
- Give the policy to employees/independent contractors and ensure compliance.
- Periodically review the policy to keep it relevant.

**Plan Ahead**

Many states have laws that require businesses to secure personal information and notify individuals of security breaches. It is, therefore, important to create a formal data security program and a policy for handling data breaches. Organizations that collect personal information from consumers in multiple states are subject to the laws of each state.

Although laws regarding data security and breach notification vary by state, there are common elements. For example, many states require businesses to designate specific employees to implement and manage their data security programs. These laws define personal information and list requirements for notifying consumers and others of data breaches. Most states also include stipulations regarding liability if a business fails to comply with laws. Some institute a private right of action that allows individuals to sue businesses for damages incurred for failing to provide timely notification of data breaches.

**Data Privacy Policy**

A privacy policy describes how a business collects, shares, safeguards, and disposes of personal information. NAR provides criteria to consider when creating a data privacy policy.

- Providing Notice to Consumers
  - Clear and prominent
  - Accessible via a direct link from each web page
  - May be revised with or without notice
- Type of Information Collected
  - Date and time of visit
  - IP address or domain name
• Statistical information about users' visits
• Type of operating system or browser used
• Voluntary information from users
• Websites visited before and after visiting the business' website

• How Information is Collected
  o Via Cookies
  o From Users

• Why Information is Collected
  o Determine how people use a business' services
  o Improve website content
  o Send notices about new products or website updates to users
  o Share with third parties including affiliates

• Handling of Information
  o Explanation about the storage of information
  o Data retention/disposal policy

• Users' Ability to Access Collected Information
  o Circumstances under which users can access information
  o Methods for dealing with users' complaints or inquiries about the handling of information
  o Instructions about how to opt-out of information collection

• Website Operator's Name and Contact Information

• Effective Date of the Privacy Policy

Summary
• Real estate businesses and professionals can take five steps to create data security programs: take stock, scale down, lock it, pitch it, and plan ahead.

• Taking stock involves performing an information inventory to determine the type of information maintained and why, who maintains and has access to the information, how information is collected, and if consumers can opt-out of the program.

• Scaling down entails (a) determining what information the business needs to gather and retain and (b) disposing of unnecessary information.

• Locking information consists of creating a data protection plan to ensure stringent safeguarding of personal information. Four key elements of a data protection plan are physical security, electronic security, employee training, and vendors' and contractors' security practices.

• Pitching information refers to properly disposing of it, which could include burning, pulverizing, or shredding paper documents and using wipe utility programs to destroy electronic files.
• Planning ahead includes creating a formal data security program and a policy that addresses the management of data breaches.

• A privacy policy describes how a business collects, shares, safeguards, and disposes of personal information.