It's 2 a.m., Do You Know What Your Data Is Doing?

The files of a real estate brokerage are a treasure trove of data, packed full of information about people and homes. When you take a look into the files that you may carry with you daily or store under lock and key in your office, the data they contain while helpful to you and necessary to the transaction could be very harmful in the hands of another. The Federal Trade Commission recommends building a sound data security plan on the following 5 Key Principles

1. Take Stock
2. Scale Down
3. Lock It
4. Pitch It
5. Plan Ahead

This course looks at those 5 Key Principles and how they relate to the day-to-day operations of a busy real estate brokerage.

Take Stock *"You don't know what you've got until it's gone…"*

Real Estate agents and Brokerages need to know what information they have, where it comes from and how they store it.

For Brokers this begins with taking a look at the brokerage as an employer:

1. What information do you collect about employees and independent contractors of the brokerage?
    - Social Security Numbers?
    - Health Insurance forms or related information?
    - Driver's License numbers or photocopies of drivers licenses?
    - Birthdate?
    - Physical address? E-mail address?
    - Telephone number?
    - Vehicle information?
2. In what manner does the brokerage receive this information?
    - A form filled out and provided to the broker?
    - A digital form filled out and provided to the broker through the office intranet?
    - A digital form filled out and provided to the broker through e-mail?
3. Where is the data stored?
    - In a filing cabinet in the office of the Broker?
    - In a filing cabinet in a general storage area?
    - In a digital file on the computer of the Broker?
    - In "the cloud"
4. How is the data secured?
    - The filing cabinet is locked?
    - The digitally stored data is encrypted?
    - It's not?
5. Who has access to the data?

- Designated employees? All employees?
- IT staff?
- 3rd Party Vendors?

Brokers and Agents need to evaluate the data they collect from clients and consumers:

1. What information do you collect about a client or consumer?
    - Social Security Number to run a credit check in the case of a short sale?
    - Photocopy of driver's license as a security precaution?
    - Physical address? E-mail address?
    - Social Media account information "handles"
    - Telephone numbers?
    - Birthdate (Everyone likes a Birthday card)
    - Photocopy of an earnest money check?
    - Mortgage application or information needed to fill out an application?
    - Home warranty application or information needed to fill out an application?
    - Employment history?
    - Divorce decree or marriage license?
    - Credit card numbers for scheduling inspections or maintenance?
2. In what manner is this information received?
    - Notes taken by an agent?
    - Forms/applications filled out by client or consumer?
    - Digital forms/applications filled out and provided through e-mail or web-site.
    - Electronic communications: e-mail, texts, instant messages, etc.
3. Where is the data stored?
    - Do agents keep copies of data separate from the files maintained by the brokerage?
4. How is the data secured?

<u>Defining Data:</u>

-Medium or Media-
Static: Paper
Digital or Electronic: Anything that requires a battery or a power cord

-Digital or Electronic-
RAM (Random Access Memory) How the data is read.
Memory: What is available when the system is powered on and running.
Storage: Where the memory goes when the system is powered down.

-Storage Form-
Magnetic: Hard drive reads magnetic discs with data in binary code
Optical: Binary code is read using light.
Flash/Solid State: Binary code is read digitally

-Defining data-
Active data: Immediately available
Archival data: "Saved data"
Latent data: Things that you didn't think were there, but are.

Scale Down

Once an audit has been performed to understand what data an agent or brokerage has, the questions "Do I need this for my business?" and "Why am I keeping this?" must be asked.

"Why am I keeping this?"

- ✓ State regulations require me to.
- ✓ My accountant told me to.
- ✓ My attorney recommended it in case of litigation.

Lock It

In determining the best way to secure data, a look at the regulation of data is recommended. There is no one federal law that regulates how personally identifiable information is to be stored; there is not one definition of personally identifiable information either. A lot of various entities regulate the security of data you maintain. Just a few are:

The FACT Act: The Identity Theft Red Flags and Address Discrepancy Rules
The Federal Trade Commission Act
47 States have some kind of law regulating data storage either data security laws or security breach notification laws.

Threats to Data
Viruses, Trojans, Worms, Drive-by-Downloads and Spyware, they all sound dangerous and they are all threats to your data, however the first step in securing your data is as simple as using the lock on your door.

IRL (In real life) Security

- ➢ Store static data and digital copies of data that contains personally identifiable information in a locked room or locked file cabinet.
- ➢ Limit access to static data and digital copies of data that contains personally identifiable information to only those employees who have a legitimate business person for doing so.
- ➢ Consider computer placement. Are screens visible to consumers? What information is displayed?

Electronic Security

Audit of office and practices:

1. What computers or servers store personal information?
2. What connections exist to those computers or servers? Internet, digital copiers, other computers in the office, smartphones, etc.
3. Do agents keep digital copies of records?
4. What applications are being used in the office and how secure are they?

Best Practices

- ✓ Install "patches."
- ✓ Run up-to-date anti-virus and anti-spyware programs on computers and servers on your network.
- ✓ Require "strong" passwords
- ✓ Install a firewall to protect computers while connected to the internet.

Devices

Laptop Security

- Brokerages should assist agents in developing laptop security protocols.
- Encrypt data on laptops
- Install "patches" regularly
- Password protection

Phones & Tablets

- Encrypt transmissions of personally identifiable information.
- Consider safety of applications
- Install updates/patches regularly
- Password protect
- Install remote wiping

<u>Cloud Storage Vendor Checklist</u>

1. <u>Security</u>
   Real Estate Licensees are entrusted with a significant amount of very private information (social security numbers, financial account information, full names, addresses) when selecting a third party vendor to store files that may contain that information, security is key.
   a. Encryption
      - What encryption methods are used to secure the data?
      - Does the vendor automatically encrypt the information when it leaves your servers and enters the cloud?
      - Who has the encryption key necessary to view that information?
      - If the vendor can access the data, are they allowed to use it?

- If the data is accessed by another party, how quickly and in what manner will the vendor notify you?

b. Physical Location
   - Where are the data servers located?
   - Who has access to the physical location?
   - What plans are in place in case of natural disaster?

c. Security Support
   - Does the vendor have security support staff that you can contact?
   - Does the vendor have independent audits of its security systems/controls?
   - Does the vendor allow for you to choose levels of security based on the data?

d. Access
   - How will you access the data?
   - How will access to the data be controlled?

2. Tech Support

   As savvy as your IT department may be, support directly from the vendor is important.
   - How and when is support available (web-chat/e-mail/telephone)?
   - Is the support staff of the vendor prepared to assist individuals with all levels of technological backgrounds and skillsets?

3. Reliability
   - How much uptime is guaranteed by the vendor?
   - Will there be times when you cannot access the data that you have stored?

4. The Fine Print

   Regardless of if you negotiate a contract with a third party vendor, or click on "agree" to a terms of use, the details of the agreement are important.

a. Money
   - Is there a set-up fee?
   - Are fees based on usage or a set amount?
   - Can the vendor increase the fees?

b. Termination
   - How can the relationship be terminated?
   - Following termination, does the vendor keep any copies to the data that was stored?

Pitch It

If there's no valid reason for documents or data to be stored, a system should be implemented to insure for timely disposal.

Paper records should be shredded or destroyed.

Destruction is the preferred method for disposing of electronic devices, it insures that no latent data will be discovered and used by a third party.

Resources

-Personal Software Inspectors-
These programs are designed to scan your system and look for outdated programs or programs that have "patches" that need applied.
Secunia
Bitdefender
FileHippo

-Encryption Programs-
Folder Lock
Dekart Keeper
PGP (pretty good protection)

-Review Web Sites-

www.toptenreviews.com

-apps to save texts-
iMazing (formerly DiskAid- primarily Apple)
PhoneView (primarily Apple)
iExplorers (primarily Apple)
CopyTrans (primarily Android/Windows)
SMS Backup & Restore (primarily Android/windows)
Tansee (primarily Apple)

-Apps That will Secure Your Texts-
textsecure
wickr
telegram
gliph