Real estate

Check yourself: A data security audit for real estate companies

Use this self-audit worksheet to learn and uphold best practices for safeguarding sensitive client information.

ShareFile™

Cybersecurity: A modern-day business imperative

It's not easy to stay on top of cybersecurity best practices in a high-stakes, fast-paced modern work environment. But for every type of organization—particularly for realtors collecting information on finances, Social Security numbers, and other data hackers would love to get their hands on—cybercrime is a very real and potentially costly threat.

According to **Statista**, the average data breach in the United States in 2023 cost $9.48 million. Financial and reputational damage typically extends months or years beyond the initial breach due to costly legal issues, fines, and customer churn. After a devastating security breach in 2019, the real estate industry giant First American agreed to pay a **$1 million penalty** to New York state. In 2023 another Fortune 500 provider of title insurance, Fidelity National Financial, was **hit with a ransomware attack** that held up home purchases across the U.S. for days, and 14.7 million people had their information leaked to cybercriminals due to a breach of the major mortgage loan servicer, Mr. Cooper.

With cybercrime being so pervasive in the industry and with so much on the line, real estate businesses must proactively work to prevent cyberattacks from occurring. But why do data breaches still happen when companies have strong security solutions?

Smarter cyber criminals

Providing password protection and virus scanning software is not enough. Today's cybercriminals are more sophisticated than ever before. A 2022 study **found** that phishing campaigns attempting to trick professionals into downloading malware or giving away sensitive information increased 61% from the previous year.

In addition to becoming more common, these attacks are becoming more calculated. Cybercriminals may send emails or texts that appear to be from a trusted source or use **topical issues** to lure their victims, with subject lines that suggest shopping deals around the holidays or fake alerts about tax filing during tax season.

AI-created malware is especially good at avoiding detection by traditional antivirus software, leading to a sharp **increase in ransomware cases** in 2023. These mounting threats from cybercriminals increase the likelihood for employees to fall into a well-conceived trap.

Preferring familiar tools and applications

With the rapid adoption of cloud-based services and proptech, real estate professionals have become more comfortable downloading and using outside applications and without informing their IT departments. While they don't mean to do any harm with this practice, known as Shadow IT, they end up bypassing security measures and putting corporate and client information in jeopardy.

Despite some awareness of the risks, many real estate professionals will continue using these unsanctioned applications because they feel familiar. It's human nature to prefer tools and applications we're already used to, and it can be difficult to adjust to working with different platforms even if they are more secure.

Working under pressure

Reluctance to adopt secure tech goes beyond the Shadow IT issue. Real estate professionals are often under pressure to adapt to market conditions, meet client expectations, stay ahead of competitors, and manage multiple time-sensitive transactions simultaneously. They need to get things done quickly without time-consuming protocols standing in their way. Adding an extra step or layer to security processes can feel too overwhelming to consider.

Steps real estate agents can take to increase data security

We understand how difficult it can be for busy real estate professionals to keep security top-of-mind while managing day-to-day operations. The security audit worksheet on the following pages outlines simple steps and features you can adopt to enhance your efficiency and boost your confidence in data security practices.

Consider returning to this audit worksheet once a quarter to make sure you're consistently following up with these recommendations. Better data security habits shouldn't feel out of reach. Even when you're pressed for time, it's important to remember that simply changing a few settings can go a long way towards providing peace of mind that client information is safe.

Audit worksheet: How can you protect customer data?

Read through the following sections and check the "Yes" or "No" boxes. At the end of this worksheet, you'll tally up the number of times you checked "Yes." This score will help you understand how effective your current data security practices are.

PART 1:

Secure files and devices

There should be no gaps in security when your real estate organization is sending, receiving, and collaborating on files with personal information or customer data. Email and file encryption scrambles text into an indecipherable format while in transit and offers protection from these bad actors, but it's only the beginning of a comprehensive security strategy.

The following questions will help you understand what steps you can take to ensure files and devices are completely secure. If you're unsure whether you have the right software to enable these recommended security features, consider checking with your IT department.

When receiving, storing, and sending files containing sensitive client information, are you:

Limiting information collection to necessary data?

□ Yes
□ No

Determining how much protection information needs and applying the right level of permissions?

□ Yes
□ No

Enabling email encryption for the body of the message and attachments?

□ Yes
□ No

Enabling file encryption to protect sensitive information in transit or at rest?

□ Yes
□ No

Utilizing custom permissions for folders and files to control who has access and for how long?

□ Yes
□ No

Enabling multi-factor authentication for more secure log-ins?

□ Yes
□ No

Avoiding the use of personal devices?

□ Yes
□ No

Enabling automated alerts that immediately flag security issues when they occur?

□ Yes
□ No

Looking at security dashboards where you can identify patterns in situations where threats are recurring?

□ Yes
□ No

In order to proactively protect customer data, do you:

Create strong, unique passwords for your accounts and devices?

□ Yes
□ No

Store passwords in a secure place?

□ Yes
□ No

Stay on top of software updates that impact the effectiveness of your security features?

□ Yes
□ No

Take an occasional free security course or read about the latest phishing threats?

□ Yes
□ No

# OF YES ________
ON THIS PAGE

PART 2:

Security and productivity

Your security tools should make it easy for you to protect clients' information while still working efficiently on their behalf. Adopting stronger, more comprehensive solutions that integrate into existing workflows is a modern-day business imperative.

If your teams lack the technological capabilities outlined below, implementing software that allows everyone to do their best work in a more secure way is essential.

When working across applications and collaborating with others, are you using:

Single sign-on capabilities to avoid repeated log-ins across apps?

☐ Yes

☐ No

Secure link sharing so your customers can access documents with one click (instead of having to download a file)?

☐ Yes

☐ No

A single, secure space such as a portal or dashboard where you can track and collaborate internally or directly with customers (as opposed to a platform that isn't secure)?

☐ Yes

☐ No

Built-in workflows for collaboration platforms that offer safe document requests and collection?

☐ Yes

☐ No

# OF YES ______

ON THIS PAGE

Your score

In the space below, tally up the number of times you checked "Yes" and put your score.

Score: _____ / 17

Assess your score against the scoring key here to analyze the strength of your current data security strategy.

**Not the score you were hoping for? It's never too late to implement best practices and strategies to better protect sensitive data. Continue refining your approach to data security and revisit this worksheet to track your progress.*

Scoring Key:

0–5 = Just getting started*

6–11 = Making progress

12–15 = Almost there

16–17 = Expert-level

Security and productivity with collaborative technology

If you scored less than 10, it could be because of your security tools' limitations.

While rigorous security practices can interfere with productivity, **they don't have to**. There are solutions available that offer both productivity and protection by embedding greater security into existing workflows.

Considering both the pressure professionals are under to work efficiently and the costly consequences of a data breach, security solutions should ensure that neither are ever compromised. Software that protects data while allowing for streamlined workflows and end-to-end productivity is well worth the investment.

Peace of mind and seamless workflows: The ideal security solution

To guarantee client data is protected, real estate companies must invest in airtight data security solutions—and employees must be able to use those tools without limiting their ability to work productively. By referring back to the above checklists, you can quickly determine what steps to take to fit security best practices into your busy work week. Both your actions and the tools you use have a real impact in preventing data breaches from happening to your organization.

Learn more about partnering with ShareFile to enhance data security through collaborative technology.