

JEANMARIE F. MOORE, CPA & SCOTT SCHINDEWOLF

Klatzkin & Co. LLP

The financial impact of a data breach

Insurance agents and brokers should be on high alert to protect client data from a cyberattack. IT security professionals, the Internal Revenue Service and media frequently disseminate warnings on new phishing schemes, ransomware and other methods that hackers use to break into systems to steal data. And, for a good reason: Cybercrime is increasing and businesses must be proactive to protect their data.

Insurance agencies that are victims of a data breach can face financial, legal and other consequences if sensitive personal and financial information is stolen on their clients. Cybersecurity needs to be taken seriously because:

- The law requires insurance agents, brokers, accountants and other professionals to protect sensitive client data.
- Clients expect you to safeguard information they entrusted you with to do your job.
- Your agency's reputation and goodwill could be compromised if there is a data breach.
- The cost of a data breach is high.
- Even one successful attack can put you out of business.

Cost of a data breach is escalating

According to a report published by IBM Security and the Ponemon Institute (*2017 Cost of Data Breach Security: United States*), the average total cost experienced by organizations over the past year increased 5 percent from \$7.01 million to \$7.36 million.

The per capita cost of a data breach is based on the number of records compromised. So, the more records that are stolen, the higher the loss. It cost companies with more than 50,000 compromised records \$10.3 million, compared to \$4.5 million for 10,000 or less stolen records.

The average cost of a data breach across all industry sectors is \$225 per capita. This number includes both direct costs of \$79 to resolve the data breach for investments in technology or legal fees, as well as indirect costs of \$146, which includes higher client turnover (churn) than in the normal course of business.

The cost of a data breach in the financial services industry is more at \$336 per compromised record. The financial services industry has the highest churn rate at 7.1 percent compared to 5.5 percent in health care and 1.9 percent in retail.

Across all industry sectors, customer turnover increased by 5 percent after a data breach.

In addition to the cost of the data breach, companies lost \$4.03 million in 2016 due to client attrition, reputation losses, diminished goodwill and increased new business development and marketing expenses.

Factors that affect the cost of a data breach

Many factors affect the cost of a data breach. Compliance failures increased the per capita cost by more than \$19 and the migration to the cloud, lost or stolen devices, third-party errors, and notifying internal and external stakeholders of the attack by \$10.

Companies can reduce the cost of a data breach loss by an average of \$9 per capita by being proactive. This includes: having a response plan; training employees on how to recognize phishing schemes and ransomware threats; putting policies and procedures in place on the use of personal computers, mobile devices and public internet access; securing passwords; encrypting data; and investing in data loss-prevention technology.

Malicious attacks are common

More than half (52 percent) of the companies that participated in the previously mentioned study experienced a malicious or criminal attack at a per capita cost of \$244, which is above the average of \$225.

Data breaches due to employee negligence or computer glitches, including IT and business process failure are less common (both 24 percent) and less costly (\$209 and \$200 per capita, respectively).

How to protect your agency


Cybercrime is not going away. Hackers are finding innovative ways to launch cyberattacks and no one is immune. Therefore, it is in your best interest to be diligent about protecting your data. Here are some recommendations:

- Audit your IT security and data protection practices annually.
- Engage an expert in the field for the audit.
- Back up your files on a regular basis.
- Train employees on cybersecurity.
- Ensure that employees are aware of new threats by cybercriminals.
- Enforce security policies and procedures to make employees accountable.
- Never allow employees to leave computers on when they are not in the office.
- Have computers go in sleep mode after a period of inactivity and require a password to sign back on.
- Don't allow employees to access client data on their personal computers or mobile devices.
- Prohibit employees from using public Wi-Fi to access the company server and data.
- Make sure that your Wi-Fi network is secure with strong passwords and encryption protocols.
- Consider "plugging in" instead of using wireless technology for certain computers, printers and scanners.

- Have a secure portal for clients to send you and access their data.
- Avoid sending or accepting sensitive client data via email.
- Password-protect and encrypt client documents.
- Implement two-factor authentication for additional login protection.
- Consider using fingerprint, eye scans and other biometric ID checks.
- Ensure your website is secure and communications protocol is HTTPS compliant.

One final note

If you receive a suspicious email, do not open an attachment or click on a link. Ransomware can hijack your data and cybercriminals may demand that you pay to get it back. According to the FBI, attackers collected more than \$209 million in ransom during the first three months of 2016. Security experts warn against paying the ransom because stolen data usually is not returned.

The best protection against ransomware is to back up data daily, keep operating systems and software up to date on all devices, invest in email, mobile and social-media security solutions and train employees. 

Moore is a certified public accountant and partner with Klatzkin & Co. LLP, and has more than 30 years of experience in the field of accounting. She is the firm's technology partner and holds the designation of Certified Information Technology Professional. Reach her at jmoore@klatzkin.com. Schindewolf is Klatzkin's IT manager. He oversees and manages the firm's IT infrastructure. Reach him at sschindewolf@klatzkin.com.



Think **PIA** first
For all your insurance needs