FACTSHEET

Common Areas of Risk in the Legal Industry

DID YOU KNOW? In 2017, more than 24,000 records were compromised in an average data breach.[1]

With so many records at risk, businesses across North America must be aware of their areas of vulnerability.

Lack of Policy

Less than 1/3 of law firms have formal cyber security training programs in place. Only 41% have formally-documented cyber security policies, incident response plans, backup and restoration procedures.[2]

Third parties

Nearly 63% of breaches are linked to third parties - 80% of law firms are not vetting their third-party service provider's data security practices.[2]

'Hactivists'

Some computer hackers promote a social or political cause by launching a cyber attack of some kind.

Ransomware

Law firms typically have the resources to pay a ransom – and may be targeted more often as a result.

Dated Equipment

Today's technology dates quickly and legacy equipment can make a law firm more vulnerable to attack.

Phishing scams

59% of all email deliveries to law firms are classified as phishing/spam emails. Phishing scams try to trick the end user into logging into a fraudulent system or downloading malware.[2]

Negligent employees

In a recent study, 54% of small and medium-sized businesses across North America and the UK showed that careless employees were the root cause of cyber security incidents.[3]

Public Wi-Fi

Attorneys often work outside of the office. Research has shown that public Wi-Fi networks, often located in cafes, libraries or other public spaces, are an especially common target for hackers.

Insiders

Changing firms is common in the legal industry and attorneys may take firm data when they leave. Other insiders, often referred to as 'rogue' employees, could steal data because they are dissatisfied.

We protect what matters.

Shred-it®

COMMON AREAS OF RISK IN THE LEGAL INDUSTRY

3 Tips to Keep Your Business Secure

Identify All Potential Areas of Risk

Conduct a walk-through of your office. Point out and mitigate any risks that you see. This will allow you to discover your pain points and solidify an information security strategy to keep data secure.

Implement Secure Workplace Policies

By establishing comprehensive policies such as a *Shred-it All* Policy and Clean Desk Policy, you encourage people to think twice about their actions in the workplace. This will push them to comply and help protect your data.

Build a Total Security Culture

Using a top down approach and integrating information security throughout the workplace, you will be able to embed it into people's everyday behavior. This will encourage them to re-consider how to securely destroy any and all confidential information.

Sources:
1. 2017 Cost of Data Breach Study, Ponemon Institute, 2017
2. Law Firm Cyber Security Scorecard, Logicforce, 2017
3. 2017 State of Cybersecurity in SMBs, Keeper, 2017

Learn more about information security in the legal industry:

877-231-0634 | shredit.com/law

Shred-it® is a Stericycle solution.

Shred-it®