FACTSHEET

Common Areas of Risk

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

There are several businesses that do not have formal information security training programs, cyber security policies, incident response plans and backup/restoration procedures in place, therefore leaving them vulnerable to a breach.

Negligent Employees

Careless employees who do not follow proper policies and procedures are the biggest risk to organizations. Sharing passwords, carrying sensitive information unnecessarily, and leaving information unattended in public places, can leave an organization at risk.

Third Parties

Businesses often share a lot of confidential information with third party vendors such as creative agencies, data analytics firms and legal professionals. With so much data being shared, it is important to consider how well third-party vendors are protecting their own data.

Insiders

Data breaches often occur as a result of privileged users abusing their rights by fraudulently transferring money or using a client's personal information to steal their identity.

Dated Equipment

As businesses incorporate new technology, systems sand software, stored or improperly-disposed of legacy assets can increase the risk of an attack.

Online Scams

Fraudsters can gain access to confidential information through business emails in order to defraud the company. They can also send emails tricking the user to download malware or log into a fraudulent system.

Digitization

With the Internet of Things (IoT) linking all devices, such as phones, cars and personal computers, it is critical to ensure that you are connected to a secure network to avoid falling victim to fraud.

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

Learn more about information security and how to keep your data secure:

800-697-4733 | shredit.com

Shred-it®