CHARLES LEACH

COMMERCIAL · PERSONAL · HEALTH · LIFE

PROTECTING YOU LIKE FAMILY.™

We've all heard the horror stories of big companies like Target and Capital One having a security breach that exposed the credit card numbers of hundreds of thousands of customers. But did you know this happens to small businesses too? Hackers know that most small businesses aren't prepared for a cyberattack, which makes them easy prey. In fact, 43% of small businesses experience cyberattacks, so it's imperative that you protect your business and your customers.

The following are the steps you should take to protect your small to mid-sized business from a cyber event:

1. Use Robust Anti-Malware and Firewall Software

Anti-virus software is NOT very effective against ransomware. Ransomware can only be detected by anti-virus tools when it is too late to save your files. While ransomware will help catch viruses when they strike, it's important to prevent them from ever entering your system in the first place.

The answer is a firewall. This will keep a virus from entering your database. Once it's installed be sure to pay attention to update notifications as they are created in response to the most current types of cyber events.

2. Encrypt and Back Up Data

An effective cybercrime protection strategy must consist of two elements: preventing physical access to sensitive data and rendering that data useless if it falls into the wrong hands. Be sure to encrypt all sensitive data, including customer information, employee information and all business data. Full-disk encryption software is included in virtually all operating systems today and can encrypt all the data on a desktop or laptop computer when it's at rest.

3. Back Up Data and Store Off Site

Backing up all data is another key way of protecting yourself from security breaches. Ransomware hackers lock companies out of their systems by encrypting their data and asking for a ransom to be paid before they release it. You can stay one step ahead of them by backing up all of your data and storing it separately.

4. Educate Employees

A. Create a security-focused workplace culture

Create a culture where all employees understand the potential devastation of a security breach and the importance of vigilantly protecting the organization. Your team should understand that cyber security training is ongoing and it will seamlessly become part of the culture of your organization.

B. Teach avoidance of unsecured websites

Staff members should be taught about the importance of never accessing unsecured websites on work devices because this gives cybercriminals direct access to sensitive data that is stored on that device, as well as browser histories and passwords.

C. Educate on the dangers of unsecured networks

Unsecured networks are often found at coffee shops, airports and hotels. These networks basically open up your system and make you vulnerable to an attack. Teach your employees to ALWAYS use a secure network when working on company business.

D. Educate employees about clicking on suspicious links

The more your employees know about cyberattacks and how to protect your data, the better off you'll be. It may be as simple as reminding them not to open attachments from people they don't know or expect.

E. Remind employees to change passwords regularly

Most employees have passwords that are too simple which makes them easy to hack. Your team members should be required to create passwords that include a combination of uppercase and lowercase letters, along with numbers and symbols. Also, you should require your employees to reset their passwords at least once a month. This will make it more difficult for hackers to infiltrate their accounts.

5. Invest In Cyber Security Insurance

43% of small businesses experience cyberattacks and 60% go out of business within 6 months of the attack, yet only 15% have cyber security insurance. Traditional policies do not cover the costs of a data security breach within your organization. Cyber insurance typically provides coverage for:

- ☑ Hotline to identify whether you've had a cyberattack
- ☑ Defense & settlement of judgment
- ☑ Forensic costs to investigate a suspected or actual breach
- ☑ Crisis management
- ☑ Fraud prevention expenses
- ☑ The costs of notifying customers
- ☑ Credit monitoring services
- ☑ Public relations
- ☑ Associated legal expenses

To learn more about how to protect your business with cyber insurance, please contact Charles Leach at **1-888-275-3224.**