5 Tips To Help Small to Mid-Sized Businesses Improve Cybersecurity

Cybersecurity threats need to be taken more seriously by businesses of all sizes! Security breaches and attacks are becoming more frequent and more impactful. But, titans of industry aren't the only ones being affected by them. Small and mid-sized businesses are also seeing an increased number of cyberattacks. One of the big reasons for this is because many small and mid-sized business owners believe that their business is too small to register on a hacker's radar. They may also believe that cybersecurity is a luxury that they cannot afford. But both of these statements are false! Small and mid-sized businesses are actually big targets for hackers because they know that their cybersecurity measures are often weak or non-existent. This makes it easier for hackers to steal personal data or perform ransomware attacks to extort money from businesses. The effects of a cyberattack can be quite devastating to small or mid-sized businesses, as they stand to lose customer confidence, credibility, trust, and a lot of money associated with the expensive process of notifying all of customers about the data breach.

Your business can greatly reduce the risk of a cyberattack by improving its cybersecurity, and below are five basic tips to get you started:

1. Keep Personal Info To A Minimum
Your liability increases as you store more personal and sensitive data. Therefore, collect and store only the information you need in order to operate. Anything else could become a liability in the event of a hack. Plus, the Federal Trade Commission (FTC) can charge you for carless storage of customer data.

2. Protect Your Data
When storing sensitive data, it is crucial to ensure that it is safe. Don't use easy to guess passwords. Make them difficult and only allow authorized users to have access to the secure data. Having a complex and difficult password is your first line of defense against hackers. Additionally, make sure to change it every few months.

3. Employee Cybersecurity Education
Lapses in cybersecurity are often due to human error. These mistakes can be avoided with simple training. Your employees should be able to accurately identify a breach and report it. They should also make sure they are accessing data in a secure location and matter.

4. Protect Payment Procedures
Credit card information is a top priority for many hackers. To combat their attacks, it's a good idea to use trusted and tested programs for processing your clients' payments. Keep payment processes with clients separate from your system in order to add another layer of security.

5. Stick With The Fundamentals
There are plenty of easy ways to protect your business. One of the first steps to take is to protect your computer systems. This means ensuring that all your computers have antivirus and antispyware programs installed and up to date. Additionally, make sure you have firewalls and spam filters up to keep out unwanted files and emails. Lastly, keep your Wi-Fi network secure and hidden to avoid unauthorized users from attempting to access it.

The Bottom Line …
Small to mid-sized businesses need to be prepared for the risky world in which we live and operate … and that's where **CISO ToGo** can help. You will find that we understand the cybersecurity needs applicable to YOUR business and we are uniquely positioned to help you satisfy them! To find out more information, check out our services listed on our website (www.CISO-ToGo.com).