FrankelZacharia LLC

Certified Public Accountants

Basic Cybersecurity Controls You Should Already Have in Place

Week after week massive data breaches remind us that pretty much all of our previous passwords are in the hands of cybercriminals. Ransomware continues to be on the rise with new twists and tools and cybercriminals are constantly looking for new ways to monetize the destruction of your business.

It seems like every day the situation is worse, but as a business owner you are not helpless.

There are basic cybersecurity controls you can put in place which will reduce the risk of loss due to a cyberattack, and they are less costly and easier to implement than you might think.

There are many tools, techniques and products available to increase your cyber defense, but these are the baseline, the least you should be doing to protect your business.

- **Understand Your Backups:** Even if you are not a "tech" person if you are responsible for an organization you should understand how your data backups work. You also need multiple backup methods, at least one of which should be somewhere in the cloud. Good backup systems can be costly, but there is nothing more important to include in your cybersecurity budget (Yes, you should have a cybersecurity budget.)

- **Multi-Factor Authentication:** Any system that can be reached from the internet, needs to have multi-factor authentication. This means if you can reach a system from the web browser without ever having to look at your phone (or some other method) then hackers are probably going to find a way in. Most of the time this is a no-cost way to increase your security.

- **Security Awareness Training:** Common sense or knowing what to do and not do are not the same thing as being aware. If you get everybody together in a group (or on Zoom) once in a while and talk about cybersecurity, your people will be more aware and this is another low-cost and easy way to increase your security. An hour of everyone's time once per year goes a long way to keeping you safe the rest of the year.

- **Phishing Testing:** Another tool to increase awareness. There are multiple vendors who have easy to use systems to provide ongoing phishing testing to your staff. Average cost is 10-20 per year per person. Not only helps identify those individuals who are "phish-prone" but also increases awareness for everyone.

- **Password Management and Education:** You can't reuse passwords. You also cannot use "pattern" passwords or anything about your hobbies, your pets, your kids or your life. If you do those things, bad things will happen. Providing a password manager is a great way to encourage better password practices.

- **Advanced Endpoint Protection:** New tools like Sentinel One and Rocket Cyber go way beyond traditional anti-virus tools and use AI and machine learning to detect and stop attacks in progress. Also an increased cost but there are versions which are budget friendly and still go a long ways beyond signature based anti-virus programs.

- **Have a Plan:** If you are a HIPAA covered entity, a Tax Preparer, financial institution or in many other industries, it is a requirement to have a risk analysis performed on a regular basis. The reason this is required is that it keeps you safer in many ways.

If you have all of these tools in place today then you are far ahead of the average small to medium sized business. If you don't, give us a shout and we would love to discuss ways to increase your cybersecurity defense plan and help you create a solid strategy for the future.