8 Practical Security Steps You Need to be Taking

Right now there is a very serious hidden war happening in the world of Cyber. A war that will affect you, if it hasn't already. Here's a list of things we implore you to ensure you are working with us to do, if you are not already.

Enable Multi-Factor Authentication

- Enable this feature on **everything** so that when you login you are prompted with a challenge and code you have to put in. Almost EVERY system does this now - turn it on, yesterday!

Implement some type of Advanced Threat Monitoring

- We are utilizing two different kinds depending on the customer need, but we CANNOT stress enough the need to actively monitor your endpoints, your entry points to your network and all of your networks traffic.

Check Microsoft Office365 Licenses

- Work with us to ensure you are using the more advanced Microsoft Office365 licenses that includes all of the advanced threat protections and security features to minimize issues.

Security Awareness Testing and Training

- Engage in regular, ongoing and automated training.The KnowBe4 software we use is doing this for many of you, but it's time to take this seriously, review the reports, talk to and counsel your staff and be sure people are paying attention.

Develop, practice, modify and update an Incident Response Plan

- This is critical and should be done together with us. This is the idea of taking a "breach mentality", meaning a mentality of not "it won't happen to us" or "if it happens to us" but instead "It will happen, and we need to be prepared!

Do the same thing with your Disaster Recovery Plan

- Using The IT Company IS NOT a DRP, it is a part of your DRP. You should absolutely spend the time with us and your team to work through what you would do to recover from a disaster.

Purchase Cyber Liability Insurance of AT LEAST 1M!

- If you don't have it now, call your agent when your done reading this and get started. We can help you navigate, but you have go to get a plan in place that covers you when something happens.

Have an ongoing Technology Plan

- Look, it's time to stop fumbling into each year hoping for the best. We have to work together to have a 12 to 36 month plan of technology assets, refreshes, projects, upgrades, removal of old technical "debt" and goals that align with your business objectives - doing this aligns directly to cyber security controls.