IT AUDIT



[...businesses cannot afford to be vulnerable to subpar data security...]

In today's digital society, businesses cannot afford to be vulnerable to subpar data security and/or support. Listed below is a short list of non-optional services that you should receive from your current IT provider. Our hope is that your current security measures up to what you need for secure business data. The threat of ransomware is on the rise, and with exposed vulnerabilities you can expect to be detected and end up paying. Are you willing to protect your business now or wait until something goes wrong?

Non-Negotiable Services

Scalability

Can your MSP scale with your company? Your MSP should guide and support you as your business continues to grow. They'll provide you with new IT strategies and products to facilitate the growth of your business. Ask your MSP if they have a security team. Do they have a hardware team? Do they have network techs or does one guy do everything? It's nice to have a great relationship with the owner-operator of the IT company, but at the end of the day, can they scale to help all their clients grow at the rate they need?

Cybersecurity

Ask your provider if they offer the latest cybersecurity measures. It's not just about technology, it's about training and staying up to date with the latest threats. Are they setting you up to train you and your staff on what to do and what not to do? Not only is your business at risk, but your employee's data, identity, and credit could also be at risk. If your IT partner isn't training you on how to identify possible threats or brief you on new threats you should probably be talking to someone else.

Internet Security

Your MSP should be taking this very, very seriously. MSPs are consistently the source of hacks and cyber-attacks because hackers know MSPs have access to their client's data. This is like a treasure chest for hackers. Ask your MSP to clearly lay out how they protect your business from security breaches. Find out what that plan is. Too loose of a security plan could make your business vulnerable and lead to a variety of issues, including lost data for you.

Poor Response Time

Too much downtime, slow response times, and not fixing the issues the first time. Ask for a report of all your service tickets for the last year. Go through them. Are they mostly reactive? Meaning, do you have to call them instead of the MSP monitoring your business. There will always be reactive tickets, but there should be a good percentage of proactive events as well. You should be receiving a report of all your backups whenever they take place.

Data Storage

Ask about your data. Where is it being stored? Is it offsite or is it in their garage? Is it in a secure data center? These days there are so many options available that your data can be anywhere. The bottom line is you need to know where it is. Do you have access to your data, or does your MSP control it? Can you perform a full restore if needed?

Network Reports

Are you getting your network summary every month? Are you aware of the good, bad, and ugly areas of your business? Ask to see the network evaluation reports that will summarize everything that went on within your business. Every workstation and every server on your network should be accounted for. As well as uptime percentage, completed backups, the number of tickets that were open, closed, and pending, and the response time. They should be giving this to you every month, either electronically or in person. And again, do they have the technology to do this?

Pricing

There's a big challenge in the MSP industry. Many times, IT companies will lure you in with a low contracted amount, yet at the end of the month, they'll surprise you by nickel and diming you for every little thing. Ask your MSP if they have a flat-rate fee. The only time you should be charged extra is if you buy something new. Flat-rate fee agreements give the MSP confidence to be your business partner, and that means they will help you grow your business. Everyone makes money when that happens!.