Invision
Computer Support for Smart Business

How an IT Security Assessment Reduces Threats to Your Business

Tim Blakely, Invision

As business owners, reading about an IT hack or stolen company and customer data gives us a queasy feeling in our stomachs. We wonder if our networks are secure. If our employees know what to do to protect information because the policies are clear. And then too quickly we shake it off and go about our day, worrying about the millions of other things it takes to run a successful business. But there are steps you can take to put your IT concerns at ease so you can focus on running your business.

IT security is a moving target that exploits vulnerabilities in both technology and people. Just when measures are put in place to fight off a new threat, another risk comes along. To continue identifying and closing gaps in your security, audits must be performed regularly to stay ahead of new phishing schemes, malware and hacker attacks. Whether you have a dedicated IT director or you outsource your IT services, an annual IT security assessment from an outside expert can provide peace of mind that you're going to pass the next technology challenge you face.

With new global threats to your IT infrastructure emerging on a daily basis, your IT security assessment should cover these key areas:

Your Network

The working remotely trend is now well established, and for many employees, it has become the status quo. However, working from home means that businesses must provide the IT support employees need to be and stay productive while keeping your data and systems safe. With more employees connecting to your network remotely, it's critical to ensure emails, messaging and other communications are managed through secure, private channels with the appropriate level of access control.

Your Hardware

Your hardware is the prime gateway to your data for hackers. Assessing your hardware means reviewing how your devices are managed at the company and employee levels. How your hardware is updated, replaced and destroyed is critical to protecting your customer and employee data.

Your Software

As soon as technology companies and software developers created devices and programs, cyber criminals emerged from the shadows to exploit any and all information they could. Their tactics grow more sophisticated every day. An assessment of your software ensures licenses are compliant and current to avoid unexpected expirations. It will also determine if programs are up to date on security and capable of protecting against known and future cyber threats.

Your Cloud Services

Cloud hosting should be assessed in line with your industry's standards. An assessment ensures that you're armed with knowledge to keep your company compliant and your data secure. Most importantly, is your backup sufficient to restore critical business functions?

Your Company Policies & Processes

Do your employees know how to spot the difference between a fake software update and a real one? Can every employee spot an email phishing scam? The best IT security in the world can't protect your data against staff who don't know how to use the tools you provide, especially in an environment incorporating remote work and a blended use of personal phones and devices. An assessment will determine how strong your company's policies and processes are so you can educate and act accordingly to boost security.

The process of undergoing a security assessment should be non-disruptive and should not alter your day-to-day operations. Once your security audit is complete, you'll have an accurate "state of the union" look at your company's current vulnerabilities and recommendations that will help you wisely allocate your IT budget for the best outcomes.