7 CRITICAL IT

SECURITY PROTECTIONS EVERY BUSINESS MUST HAVE IN PLACE

TEKconn

If your business is the victim of a cybercrime attack where client or patient data is compromised, what would you do?

Many business owners are shocked when they get compromised because they believed their IT had it "handled." However, there is an army of thousands of hackers and sophisticated crime rings that work around the clock to bypass known protections – and you can't stop a brand-new threat that was invented today with a security system that was designed a week ago let alone a year ago. It requires special expertise to stay on top of all of this, which is why many don't.

Here's a 7 step list. If your company isn't actually implementing all of these protocols or if you don't know if you are − Why not?

1.The #1 security threat to any business

Are employees! Like it or not, almost all security breaches in business are due to an employee clicking, downloading or opening a file that's infected, either on a website or in an e-mail; once a hacker gains entry, they use that person's e-mail and/or access to infect all the other PCs on the network. Phishing e-mails (an e-mail cleverly designed to look like a legitimate e-mail from a website or vendor you trust) are still a very common occurrence – and spam filtering and antivirus cannot protect your network if an employee is clicking on and downloading the virus. That's why it's critical that you educate all of your employees in how to spot an infected e-mail or online scam. All it takes is one accident, consistent reminding and educating your employees is critical.

On that same theme, the next precaution is implementing an Acceptable Use Policy. An AUP outlines how employees are permitted to use company-owned PCs, devices, software, Internet access and e-mail. We strongly recommend putting a policy in place that limits the websites employees can access with work devices and Internet connectivity.

Further, you have to enforce your policy with content-filtering software and firewalls. We can set up permissions and rules that will regulate what websites your employees access and what they do online during company hours and with company owned devices, giving certain users more access than others.

With so many applications in the cloud, an employee can access a critical app from any device with a browser, considerably exposing you to risks.

If an employee is logging in to critical company cloud apps through an infected or unprotected, unmonitored device, it can be a gateway for a hacker to enter your network – which is why we don't recommend you allow employees to work remote or from home via their own personal devices.

Second, if that employee leaves, are you allowed to erase company data from their phone or personal laptop? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to ensure yourclients' information isn't compromised?

Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured, but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

2. Require strong passwords and passcodes to lock mobile devices.

Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, this can be enforced by your network administrator so employees don't get lazy and choose easy-to-guess passwords, putting your organization at risk. Are they? If you and your employees are not being forced to do a password reset every 30-60 days, they fail best practices.

3. Keep your network and all devices patched and up-to-date.

New vulnerabilities are frequently found in common software programs you are using, such as Adobe, Flash, Microsoft or QuickTime; therefore it's critical you patch and update your systems and applications when patches become available. If you're under a managed IT plan, this can all be automated for you so you don't have to worry about an employee missing an important update.

4. Have a business-class image backup both on-premise & in the cloud.

This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, and against natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be automated and monitored; the worst time to test your backup is when you desperately need it to work.

5. Don't allow employees to access company data with personal devices that aren't monitored and secured by your IT department.

The use of personal and mobile devices in the workplace is exploding. Thanks to the convenience of cloud computing, you and your employees can gain access to pretty much any type of company
data remotely; all it takes is a known username and password. Employees are now even asking if they can bring their own personal devices to work
(BYOD) and use their smartphone for just about everything. But this trend has drastically increased the complexity of keeping a network and your company data secure.

If you are allowing employees use personal devices and home PCs, you need to make sure those devices are properly secured, monitored and maintained by a security professional. Further, do
not allow employees to download unauthorized software or files. One of the fastest ways cybercriminals access networks is by duping unsuspecting users into willfully downloading malicious software by embedding it within downloadable files, games or other "normal"
looking apps. But here's the rub: most employees won't want you monitoring and policing their personal devices; nor will they like that you'll wipe their device of all files if it's lost or stolen. But that's exactly what you'll need to do to protect your company. Our suggestion is that you allow employees to access work-related files, cloud applications and e-mail only via company-owned and monitored devices, and never allow employees to access these items on personal devices or public WiFi.

Mark Twain Once Said, "Supposing Is Good, but Knowing Is Better"

If you want to know for sure that your current IT company (or IT person) is truly doing everything they can to secure your network and protect you from ransomware, bank fraud, stolen and lost data and all the other threats, problems and costs that come with a data breach, then you need to call us for a complimentary Security And Backup Audit. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of the audit, a few things you'll learn:

• Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?

• Is your data backup truly backing up all the important files and data you would never want to lose – and how fast could you get your IT systems back online if hit with ransomware? Most businesses are shocked to learn it will take much longer than they anticipated).

• Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are outside of your backup?

6. A business grade firewall & routine updates.

A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network, or they are completely useless. This too should be done by your IT person or company as part of their regular, routine maintenance. However it's not uncommon for an IT guy to forget to turn on one or more of the intrusion detection and prevention features; often they are disabled to work on the firewall, but then never turned back on, making the device useless.

Get the facts and be certain your business, your reputation, and your data is protected.

7. Protect your bank account.

Did you know your business' bank account doesn't enjoy the same protections as a personal bank account? For example, if a hacker takes money from your business account, the bank is not responsible for getting your money back. (Don't believe me? Go ask your bank what their policy is on refunding you money stolen from your

account!) Many people think FDIC protects you from fraud; it doesn't. It protects you from bank insolvency, not fraud.

So here are three things you can do to protect your bank account. First, set up e-mail alerts on your account so you are notified any time money is withdrawn. The faster you catch fraudulent activity, the better your chances are of keeping your money. In most cases, fraudulent activity caught the day it happens can be stopped. If you discover it even 24 hours later, you may be out of luck. That's why it's critical that you monitor it daily and contact the bank immediately if you see any suspicious activity.

Want Help In Implementing These Essentials?

Contact Our Team of Experts For A Zero Obligation Consultation

CONNECT TODAY

800-955-0231

info@tekconn.com

TEKconn