10 Essential Security Protections Every Business Should Have In Place

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim! This report will get you started in protecting everything you've worked so hard to build.

Provided By: Z-JAK Technologies
Author: Jeff Chandler

https://zjak.net
(502) 200-1169
info@zjak.net

Small Businesses are Under Attack!

Right now, extremely dangerous and well-funded cybercrime rings in China, Russia and the Ukraine are using sophisticated software systems to hack into thousands of small businesses like yours to steal credit cards, client information, and swindle money directly out of your bank account. Some are even being funded by their own government to attack American businesses.

Don't think you're in danger because you're "small" and not a big target like a J.P. Morgan or Home Depot? 82,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at small businesses; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits, data-breach fines and out of sheer embarrassment.

In fact, the National Cyber Security Alliance reports that **one in five** small businesses have been victims of cybercrime in the last year – and that number is growing rapidly as more businesses utilize cloud computing, mobile devices and store more information online. You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity. **Because of all of this, it's critical that you have these 10 security measures in place.**

1. **Train Employees on Security Best Practices.** The #1 vulnerability for business networks **are the employees** using them. Since almost all cyber security breaches were founded in human error (someone clicking on a link in an e-mail, accidentally downloading a virus, falling for a phishing scam), we strongly recommend you provide all employees cyber security awareness training that not only teaches them how to spot a scam, but also conducts simulated phishing tests to see if what they've learned actually "sticks" and is being used.

2. **Create an Acceptable Use Policy (AUP) – And Enforce It!** 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 web sites employees can access with work devices and Internet connectivity. Further, you must enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what web sites your employees access and what they do online during company hours and with company-owned devices, giving certain users more "freedom" than

others.

Having this type of policy is particularly important if your employees are using their own personal devices to access company e-mail and data.

If that employee is checking unregulated, personal e-mail on their own laptop that infects that laptop, it can be a gateway for a hacker to enter YOUR network. If that employee leaves, are you allowed to erase company data from their phone? 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 YOUR clients' information isn't compromised?

Further, if the data in your organization is extremely 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.

3. **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 choose easy-to-guess passwords, putting your organization at risk.

4. **Keep Your Network Up to Date.** New vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office; therefore, it's critical you patch and update your systems frequently. If you're under a managed IT plan, this can all be automated for you, so you don't have to worry about missing an important update.

5. **Have an Excellent Backup.** 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, 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!

6. **Don't Allow Employees to Download Unauthorized Software or Files.** One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games, or other "innocent"-looking apps. This can largely be prevented with a good firewall, updated anti-virus software and employee training and monitoring.

7. **Don't Scrimp on A Good Firewall.** 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. This too should be done by your IT person or company as part of their regular, routine maintenance.

8. **Use Encrypted E-mail for Confidential Information** - Breach, privacy and notification laws, along with "best efforts" and "reasonable care" standards, put the burden of vigilance and guardianship of personally identifiable and confidential information on you. Since e-mail is a highly unsecure way of sending PII (personally identifiable information) such as health-related information or medical records, social security numbers, credit card, banking, or financial information, it's essential to have e-mails encrypted to prevent the contents from being read by anyone other than the intended recipients.

   We strongly encourage a more extensive and robust assessment be done immediately to determine what, if any, exposure you may have. Sensitive data can be automatically encrypted based on the type of data contained in the message, or manually encrypted by the sender. We recommend automatic encryption so that sensitive information isn't accidentally e-mailed in "plain text" due to human error.

9. **Purchase Cyber Liability Insurance.** Even organizations that implement strong security policies run the risk of a data breach. Some data breaches occur due to employee misconduct (intentional or unintentional), computer viruses, phishing scams, etc. Breaches of non-public information (NPI) can be costly due to breach reporting requirements, remediation services including information technology, forensics, legal, credit monitoring and possible regulatory fines. Cyber insurance can offset the expenses of NPI related data breaches.

10. **Implement a Clean Desk Policy.** One of the simplest security principles you can instantly implement is a "clean desk" policy that requires employees to clear their desk of any files, folders or papers containing sensitive information before walking away. Implementing this policy is recommended even for employees that work from home.

    Once such a policy is in place, it is important to make certain the policies are, in fact, being followed. If you're working in an office environment, we recommend having someone periodically check desks after hours or during lunch breaks to ensure your team is following this policy and to ensure compliance. For work from home staff, regular reminders of the policy to your team are recommended.

Want Help In Implementing These 10 Essentials?

If you are concerned about employees and the dangers of cybercriminals gaining access to your network, then call us about how we can implement a managed security plan for your business.

At no cost or obligation, we'll conduct a free **Security and Backup Audit** of your company's overall system health to review and validate potential data-loss and security loopholes, including fine-print clauses used by all 3rd-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs.

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a 3rd party to validate nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you.

You Are Under No Obligation To Do Or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our **Free Security and Backup Audit**. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.

Whether or not we're a right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to give this free service to you.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected. Call us at **502-200-1169** or you can e-mail me personally at **jeff@zjak.net**.

Dedicated to serving you,

Jeff Chandler

Web: https://zjak.net
E-mail: jeff@zjak.net

