STRATiiS

7 Urgent Security Protections Every Business Should Have In Place

Provided by: Stratiis Ltd
Author: Alun Borland
W: www.stratiis.com
T: 0141 348 7960

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are 'low hanging fruit'.

This report will get you started in protecting everything you have worked so hard to build.

Are You A Sitting Duck?

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 utilise 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 7 security measures in place.

7 Ways To Protect Your Business

1. **Train Employees on Security Best Practices.** The #1 vulnerability for business networks are the employees using them. It's extremely common for an employee to infect an entire network by opening and clicking a phishing e-mail (that's an e-mail cleverly designed to look like a legitimate e-mail from a web site or vendor you trust). If they don't know how to spot infected e-mails or online scams, they could compromise your entire network.

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 websites employees can access with work devices and internet connectivity and enforce your policy with content-filtering software and firewalls. We can easily 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 "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?

If the data in your organisation 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.

3. **Require Strong Passwords and Pass Codes to Lock Mobile Devices.** Passwords should be at least eight characters and contain lowercase and uppercase letters, symbols and at least one number. On a mobile phone, requiring a pass code to be entered will go a long way toward preventing a stolen device from being compromised.

4. **Keep Your Network Up-To-Date.** New vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office; 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 to get them back. A good backup will also protect you against an employee accidentally deleting or overwriting files, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Your backups should be automated and monitored.

6. **Don't Allow Employees to Download Unauthorised Software or Files.** One of the fastest ways cyber-criminals 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 and employee training and monitoring.

7. **Don't Scrimp on A Good Firewall.** A firewall acts as the front-line 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.

Looking For Support in Implementing These 7 Essential Steps?

We can help! Our expert team are on hand to guide you through the process, just give us a call to find out how we can implement a managed security plan for your business.

At no cost or obligation, we'll send one of our security consultants to your office to conduct a free Security and Backup Audit of your company's overall network health to review and validate data-loss and security loopholes. 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 this free audit, you'll know:

- Is your network really and truly secured against the most devious cyber-criminals? And if not, what do you need to do (at a minimum) to protect yourself now?
- Is your data backup truly backing up all of the important files and data you would never want to lose? We'll also reveal exactly how long it would take to restore your files.
- Are you accidentally violating any data-privacy laws? New laws are being put in place frequently and it's easy to violate one without even being aware.
- Is your firewall and antivirus configured properly and up-to-date?
- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are outside of your backup?

No Obligation Audit

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. If we are the right fit for you, we'll welcome the opportunity and if not, we're still more than happy to offer you this complimentary service.

If you would like to chat through this opportunity, please call us directly at **0141 348 7960** or you can e-mail me personally at **aborland@stratiis.com** .