7 Urgent Security Protections Every Business Should Have In Place Now

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: Vermont Systems Ltd
Author: Chris Ward

Vermont Systems Ltd, *IT Support and Services*
Speedwell House
Speedwell Close
Chandlers Ford
Hampshire
SO53 4BT

Phone: 023 8098 3405
E-mail: chris.ward@vermont.co.uk

Are You A Sitting Duck?

You, the CEO of a small business, 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 swindle money directly out of your bank account.

Don't think you're in danger because you're "small" and not a big target like a Sony or VTech? Think again. 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 Federation of Small Businesses (FSB) reports that small businesses in the UK lost £785 million in 12 months, and 41% of FSB members had been victims of cyber crime. 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 7 security measures in place.**

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) or cleverly disguised attachment. 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 web sites employees can access with work devices and Internet connectivity. Further, you have to 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 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. **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.

4. **Backup is easy. You need fast and reliable recovery.** 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!

5. **Keep ALL of your data safe** If your staff don't put the data where you asked them, it isn't safely backed up. And from what we see every day, they aren't. And the more senior they are, the less likely they are to do it. And ironically, this means that the most valuable data is most at risk. Busy sales people want to get access to files from home or at a client's office. Hardworking project teams will work from home in the evening to meet deadlines.

   So files end up in personal Dropbox accounts, or saved directly onto a laptop. This means they aren't backed up and when the ransomware hits … bang … they are gone (and beyond this it is out of your control if they leave the business). So firstly checking where files are stored, and providing reliable and flexible access to your IT systems will facilitate productive AND safe working.

6. **Don't allow employees to download and install 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 be prevented with a good firewall, correct PC configuration and employee training and monitoring.

So make sure the PCs are updated with the latest Windows and other updates. This plugs the gaping security holes Microsoft, Adobe and the others didn’t fix first time around. These updates come out at least monthly and should be applied straight away (once it is available, the bad guys are alerted to start exploiting it)

And remove your users “admin” privileges from their PC. Too many people still have this in place, and it means the user can install software and make changes. And this means that the malware can too.

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 not all firewalls are created equal. Good ones will filter your internet traffic for nasties and block threats than standard Antivirus and other prevention doesn’t stop. 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.

Want Help In Implementing These 7 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 send one of our security consultants and a senior, certified technician to your office to conduct a free **Security And Backup Audit** of your company’s overall network health to review and validate as many as 31 different data-loss and security loopholes, including small-print weasel 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. At the end of this free audit, you’ll know:

- 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? We’ll also reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).

- Are your employees freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social media

sites? You know some of this is going on right now, but do you know to what extent?

- Is your firewall and antivirus configured properly and up-to-date? Is it setup to block common threats which will bring your system to a standstill such as CryptoLocker or Cryptowall?

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

I know it's natural to want to think, "We've got it covered." **Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the 100s of businesses we've audited over the years.**

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? Get the facts and be certain your business, your reputation and your data are protected. Call us on 023 8098 3405 and ask to speak to Chris, Oliver or John. Or you can e-mail me personally at chris.ward@vermont.co.uk.

Dedicated to serving you,

Chris Ward
Web: www.vermont.co.uk
E-mail: chris.ward@vermont.co.uk

Here's What A Few Of Our Clients Have Said:

"Vermont had the vision to see where we were headed…"

Running an investment specialist IFA needs complex integration of numerous databases and systems.

Vermont stepped in at an early stage of our development and had the vision to see where we were heading, maximise our operational capacity within a tight budget and ready us for our expansion.

At all stages Vermont has remained in close communication, tackling any problems cheerfully and efficiently.

Richard Palmer
Senior Planner, Murdoch Asset Management

"Vermont help us achieve our goals"

We've set ourselves ambitious plans for business expansion and we are confident that Vermont will provide their support and guidance to help us achieve them – this is a long-term relationship offering long-term benefits all round.

Sarah Key
Office Manager
Turbo Service International

"Vermont help us budget and plan for the future"

Vermont take the time to find out where we are going as a business and help us understand how our IT system can cope with the changes to budget and plan for the future.

Tom Noyce
M.D. Noyce Insurance