7 URGENT SECURITY PROTECTIONS EVERY BUSINESS SHOULD HAVE RIGHT NOW

Cybercrime is at an all-time high. Hackers are setting their sights on small and medium businesses that 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.

powersolution.com
your one IT solution

445 Godwin Ave., Ste 2, Midland Park, NJ 07432 **Call: 201-493-1414 x 301**

ARE YOU A SITTING DUCK?

Your small business is under attack. **Right now, extremely dangerous and well-funded cybercrime rings** in China and Russia among other countries are using sophisticated software systems to **hack into *thousands* of small businesses like yours** to steal credit cards and client information and to swindle money directly from your bank account. Some are even funded by their own government to attack American businesses.

Think you're not in danger because your business is "small" and not a big target like a J.P. Morgan or Home Depot? Think again. Over 90,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at small businesses. **You don't hear about most of the attacks because they are kept quiet for fear of generating 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 past years – and that number is growing rapidly as more businesses utilize cloud computing, deploy 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 severity and number respectively.

Because of all these threats, it's critical that you have the following 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). 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 Internet connectivity and the web sites employees can access with work devices. Further, you have to enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that 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 an employee is checking unregulated, personal e-mail on their personal laptop and an email attack infects that laptop, this can be a gateway for a hacker to enter YOUR network. If an 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. 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 thereby putting your organization at risk.

4. Keep Your Network Up-To-Date. New vulnerabilities are frequently found in common software programs such as Microsoft Office; therefore, it's critical that 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 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 or install Unauthorized Software or Files. One of the fastest ways cybercriminals access networks is by duping unsuspecting users into downloading hidden malicious software embedded 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 Skimp 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.

WANT HELP IN IMPLEMENTING THESE 7 ESSENTIALS?

If you are concerned about employees and the dangers of cybercriminals gaining access to your network, you need to make sure there is a managed security plan implemented for your business.

Just how sure are you about answering these questions:

- Is your network **really 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).
- Can your business be **compromised by your employees**? Are your staff members freely using the Internet to access gambling sites and porn, to look for other jobs, and waste time shopping? Do they 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?
- Are you **accidentally violating** any PCI, HIPAA or other data-privacy laws? New laws are being put in place frequently and it's easy to violate one without even being aware; however, you'd still be subject to the bad PR and fines.
- 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?

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 small and medium size 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. We have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, we'll report it to you.

YOU ARE UNDER NO OBLIGATION TO DO OR BUY ANYTHING

Let's have a conversation about potential 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. Let's talk about common places where security and backup get overlooked, such as mobile devices, laptops, tablets, and home PCs.

During our free consultation you won't have to deal with a pushy, arrogant salesperson – we don't appreciate heavy sales pressure any more than you do.

Whether or not we're the 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 have a discussion about your business security with 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 201-493-1414 today – we are dedicated to serving you.

Contact: David Dadian, CEO
Email: david@powersolution.com
Phone: (201) 493-1414 x 301
Web: https://powersolution.com/

HERE IS WHAT A FEW OF OUR CLIENTS HAVE SAID:

Immediate and reliable services every time we needed them

The team at powersolution.com has provided us with immediate and reliable service every time we needed them. It is a comfort knowing that their preventive IT solutions are always working behind the scene, allowing us to focus on what's important, the business of serving emergency responders with the equipment they need to save lives…

- Vernon Ralph, CEO V.E.Ralph/Emergency Medical Products, Kearny, NJ

They are professionals

The powersolution.com team has given us the straight talk on what we need, cost-effective solutions and detailed proposals. Their IT methods are always seamless, never interrupting our operations and, at the best cost. When we've asked, they have delivered. I would recommend them to any business that needs a dependable and reliable IT support team. They are professionals.

- Michael Elkas, Pres., Atomizing Systems Inc, Ho-Ho-Kus, NJ

They don't just build solutions, they build relationships

When we were looking for an e-commerce solution, powersolution.com's web staff was there to help us transfer our ideas into reality. Their creative guidance and understanding of our business were essential in getting out our message. Leaving room for expansion of the site, they worked diligently to make sure the results were accomplished within our budget. powersolution.com stays in touch from the start to the finish of a job. They don't just build solutions, they build relationships.

- Tom Nizza, President, MTM Resources, Hackensack NJ