7 CRITICAL IT SECURITY PROTECTIONS EVERY BUSINESS SHOULD HAVE IN PLACE NOW

Provided by:
Robert Cleary
President/CEO
508-205-1114
www.ClearComIT.com

ClearCom IT Solutions

Cybercrime is at an all-time high, and 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.

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 Ukraine are using sophisticated software systems to hack into thousands of small businesses like yours to steal credit cards and 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? Think again. 230,000 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 47% of small businesses had at least one cyberattack in the past year, 44% of those had 2-4 attacks – and that number is growing rapidly as more businesses utilize cloud computing, mobile devices and store more information online..

47% OF SMALL BUSINESSES HAD AT LEAST ONE CYBERATTACK IN THE PAST YEAR

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 is 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 website 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 Acceptable Use Policy 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 easily set up permissions and rules that will regulate what websites your employee's 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 that infects that phone or 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 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.

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.

Simply having a solid, reliable backup can foil some of 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!

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 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 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 IN YOUR ORGANIZATION?

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 **Cybersecurity Risk Assessment** of your company's overall network health to review and validate different data-loss and security loopholes, such as 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 ASSESSMENT, YOU'LL KNOW:

- IF your IT systems and data are truly secured from hackers, cybercriminals, viruses, worms, and even sabotage by rogue employees. 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 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 have to suffer the bad PR and fines.

- If you and your employees' credentials, passwords, and private information are being sold on the Dark Web (I can practically guarantee they are, and the information we dig up will shock you).

- IF your IT systems, backup, and data handling meet strict compliance requirements for data protection.

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 many 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

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 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 508-205-1114, request your free cybersecurity assessment online at https://www.clearcomit.com/risk-assessment/ or you can e-mail me directly at **team@clearcomit.com**.

Dedicated to serving you,

Rob Cleary
Phone: 508-205-1114
Web: www.ClearComIT.com

Request your Free Cybersecurity Assessment online at https://www.clearcomit.com/risk-assessment/

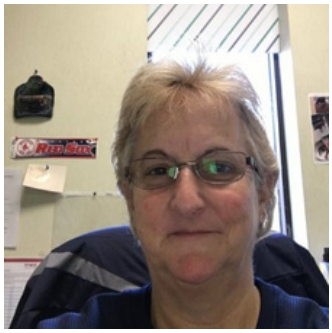
HERE'S WHAT A FEW OF OUR CLIENTS HAVE SAID:

Saved Us from Hundreds of Hours of Downtime

"ClearCom IT's help-desk and remote capabilities have **freed up a tremendous amount of my time** that used to be spent troubleshooting with an IT professional on the phone. In the 5 years I've worked with ClearCom IT Solutions they have always been professional and prompt. Every time I call for support, a knowledgeable IT professional **answers the call** and ensures that my issue is resolved. Their remote support staff has saved us hundreds of hours of downtime. **For our mid-size company that has no on-site IT support, ClearCom IT Solutions offers exactly what we need.**"

Don Sauer – VP of Finance - Sanderson Macleod, Inc.

Outperforms the Competition, While Still Being Cost-Effective



"ClearCom IT **offers more services for our money,** which is a huge benefit for our manufacturing company. Unlike other IT providers we've worked with in the past, their efficacy in correcting any problems or situations that we encounter has **reduced downtime** for our organization. After researching and comparing many IT companies, ClearCom IT outperforms the competition with **exceptional professionalism and knowledge** while still being cost-effective. "

Nancy Belham – President, Bell's Powder Coating, Inc.

Complete trust & Confidence

"We were initially hesitant to change IT companies because we didn't want to go through the pain of switching providers. However, **the transfer over to ClearCom IT Solutions was so much easier than we anticipated**. ClearCom IT has been absolutely stellar on all levels. I cannot say enough good things about them. We have complete trust & confidence that the team will handle our issues with the utmost care & in a very timely response. Our Staff Is Thrilled!!

If you want an IT partner who **responds to your needs quickly and actually FIX your issues**, not just band-aid them together, give ClearCom IT a call. Their team is the best!

Jennifer Vibber – Office Manager - Spear Management Group, Inc.