7 Crucial Security Measures SMBs *Should* Have In Place

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium-sized businesses who are "low hanging fruit."
Don't be their next victim!

CORPORATE TECHNOLOGIES GROUP

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 and Russia 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. Their own government is even funding attacks on small, virtually defenseless businesses.

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

According to Verizon's 2025 Data Breach Investigations Report, third-party involvement in breaches has doubled, rising from about 15% to 30% of all confirmed breaches. For SMBs, this means risk doesn't just come from your own systems, but also from vendors, partners, and service providers that may be less secure. Quite simply, most small businesses are low-hanging fruit to hackers due to their lack of adequate security systems. and the complex web of third-party connections they rely on.

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 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.

To Request Your FREE Network Assessment On One Of Your Networks, Visit Our Website At **https://ctgusa.net/free-network-assessment/** or call 330-655-8144.

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. Furthermore, 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 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 email and data. If that employee is checking unregulated, personal email on their own laptop and it is infected, 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 the employee's photos, videos, texts, etc. – to ensure YOUR clients' information isn't compromised?

Even 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 12 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.

To Request Your FREE Network Assessment On One Of Your Networks, Visit Our Website At **https://ctgusa.net/free-network-assessment/** or call 330-655-8144.

4 Keep Your Network Up-To-Date

New vulnerabilities are frequently found in common software programs you are using, such as Microsoft 365; 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 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 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.

To Request Your FREE Network Assessment On One Of Your Networks, Visit Our Website At **https://ctgusa.net/free-network-assessment/** or call 330-655-8144.

Want Help 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 Network Assessment to review and validate data-loss and security loopholes, including small-print weasel clauses used by all third-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We can 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 have these questions answered:

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?

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.

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

Is your firewall and antivirus configured properly and up-to-date?

To Request Your FREE Network Assessment On One Of Your Networks, Visit Our Website At **https://ctgusa.net/free-network-assessment/** or call 330-655-8144.

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 hundreds 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 third 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 Network Assessment.

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 330-655-8144, or you can e-mail me personally at brett.harney@ctgusa.net

Dedicated to serving you, Brett Harney
Web: www.ctgusa.net
E-mail: brett.harney@ctgusa.net
Phone: 330-655-8144

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

From Frustration to Seamless Communication with CTG

CTG has been a valued service vendor to Impact Ind. for well over 5+ years. We previously had trouble with our equipment and service prior to switching to CTG. Their entire staff at CTG made the transition to new equipment and service a simple one. The products we have had installed are easy to use and work extremely well in meeting our needs. We appreciate the quality of service we are provided by CTG's staff, making our phone and communication systems virtually hands off and simple to use. In today's competitive manufacturing market, having proper communication is the key to success. Not having to worry about phones, fax, and internet services is priority and CTG has made this possible. Laura Kaiser has gone above and beyond to ensure all our needs are met. She does a fantastic job! CTG has a fantastic group of people and can provide top notch service.

- **H. Britt, Impact Industries**

A Smooth Upgrade Without the Stress

CTG guided us through the delicate process of replacing a failing 30-year-old analog phone system that was not only heavily integrated into other hardware, but also dear to many employees. CTG's staff researched options, presented only what we needed, and provided us with attentive and understanding staff for the transition.

- **J. Hunter, Nerone and Sons**

A Smooth Upgrade Without the Stress

We faced significant challenges during our move to a new building earlier this year, requiring a complete overhaul, including a new phone system, and wiring the entire facility for IT and phones. When surprises beyond their control happened (which they do in every project), they were able to come up with alternate solutions. Their excellent project management skills and "can do" attitude helped us get up and running when we needed to be. I choose to work with CTG because they have a good reputation in the industry and are good at what they do

- **B. Centa, PMI Industries**

Project Challenges Solved with a 'Can Do' Attitude

I and the companies I have worked for have been clients of Corporate Technologies Group for over twenty plus years. The years we have been associated with CTG speaks to our confidence in their ability to support our communications and data needs. As our needs have evolved, so has CTG's ability to provide state-of-the art solutions to meet those needs. For me, CTG has provided a single source for communications products and especially support. When support issues come up, one call to CTG and I am done. CTG's staff see the issue through to its resolution and keep me informed of their progress. Thank you CTG!

- **E. Ardale, Manchester, Newman, & Bennett L.P.A.**

To Request Your FREE Network Assessment On One Of Your Networks, Visit Our Website At **https://ctgusa.net/free-network-assessment/** or call 330-655-8144.

To Request Your FREE Network Assessment:

1. Go online to https://ctgusa.net/free-network-assessment
2. Call us direct at 330-655-8144
3. E-mail your appointment request to info@ctgusa.net

CORPORATE TECHNOLOGIES GROUP