The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks

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: Parallel Edge, Inc.
Author: Sondra Lorino
126 E. Beechtree Lane, Wayne PA 19087
Paralleledge.com 610.293.0101

Are You Vulnerable?

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 steal credit cards, 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. 82,000 NEW malware and ransomware 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 one in five small businesses have been victims of cybercrime in the last year – and that number is growing rapidly as more businesses utilize cloud computing and 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. **The #1 Security Threat To ANY Business Is...** Humans! Like it or not, almost all security breaches in business are due to an employee clicking, downloading or opening a file that's infected, either on a web site or in an e-mail; once a hacker gains entry, they use that person's e-mail and/or access to infect all the other PCs on the network. Phishing e-mails (e-mails cleverly designed to look like legitimate messages from a web site, a vendor you trust, or even someone inside your organization) is a very common occurrence – and **spam filtering and anti-virus cannot protect your network if an employee is clicking on and downloading the virus.** That's why it's CRITICAL that you educate all your employees on how to spot an infected e-mail or online scam. Cybercriminals are EXTREMELY clever and can dupe even sophisticated computer users. All it takes is one slip-up; so constantly reminding and educating your employees is critical.

   On that same theme, the next precaution is implementing an Acceptable Use Policy (AUP). 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 and home computers to access company e-mail and data. With so many applications in the cloud, an employee can access a critical app from any device with a browser, which exposes you considerably.

If an employee is logging into critical company cloud apps through an infected or unprotected, unmonitored device, it can be a gateway for a hacker to enter YOUR network – which is why we don't recommend you allow employees to work remote or from home via their own personal devices unless it has the recommended anti virus, monitoring, and Managed Services installed.

Second, if that employee leaves, are you allowed to erase company data from their phone or personal laptop? If their phone is lost or stolen, can you, and 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 and cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

2. **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.

3. **Keep your network and all devices patched and up-to-date.** New vulnerabilities are frequently found in common software programs you are using, such as Adobe, Flash or QuickTime; therefore, it's critical you patch and update your systems and applications when one becomes available. If you're under a Managed Services plan, this can all be automated for you so you don't have to worry about missing an important update.

4. **Have An Excellent Backup.** This can foil the most aggressive 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. **Don't allow employees to access company data with personal devices that aren't monitored and secured by YOUR IT department.** The use of personal and mobile devices in the workplace is exploding. Thanks to the convenience of cloud computing, you and your employees can gain access to pretty much any type of company data remotely; all it takes is a known username and password. As you are probably aware, employees are asking if they can bring their own personal devices to work (BYOD) and use their smartphone for just about everything, but this trend has DRASTICALLY increased the complexity of keeping a network – and your company data – secure. In fact, your biggest danger with cloud computing is not that your cloud provider or hosting company will get breached (although that remains a possibility); your biggest threat is that one of your employees accesses a critical cloud application via a personal device that is infected, thereby giving a hacker access to your data and cloud application.

   So, if you ARE going to let employees use personal devices and home PCs, you need to make sure those devices are properly secured, monitored and maintained by a security professional. Further, do not 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.

But here's the rub: Most employees won't want you monitoring and policing their personal devices; nor will they like that you'll wipe their device of all files if it's lost or stolen. But that's exactly what you'll need to do to protect your company. Our suggestion is that you only allow employees to access work-related files, cloud applications and e-mail via company-owned and monitored devices, and never allow employees to access these items on personal devices or public WiFi.

6. **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 or they are completely useless. This too should be done by your IT person or company as part of their regular, routine maintenance.

7. **Protect Your Bank Account.** Did you know your COMPANY'S bank account doesn't enjoy the same protections as a personal bank account? For example, if a hacker takes money from your business account, the bank is NOT responsible for getting your money back. (Don't believe me? Go ask your bank what their policy is on refunding you money stolen from your account!) Many people think FDIC protects you from fraud; it doesn't. It protects you from bank insolvency, NOT fraud.

   So here are 3 things you can do to protect your bank account. First, set up e-mail alerts on your account so you are notified any time money is withdrawn. The FASTER you catch fraudulent activity, the better your chances are of keeping your money. In most cases, fraudulent activity caught the DAY it happens can be stopped. If you discover it 24 hours after it's happened, you may be out of luck. That's why it's critical that you monitor your account daily and contact the bank IMMEDIATELY if you see any suspicious activity.

   Second, if you do online banking, dedicate ONE computer to that activity and never access social media sites, free e-mail accounts (like Hotmail) and other online games, news sites, etc. with that PC. Remove all bloatware (free programs like QuickTime, Adobe, etc.) and make sure that machine is monitored and maintained behind a strong firewall with up-to-date anti-virus software. And finally, contact your bank about removing the ability for wire transfers out of your account and shut down any debit cards associated with that account. All of these things will greatly improve the security of your accounts.

ParallelEdge

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.

We'll send one of our security consultants to your office to conduct a **Security And Backup Audit** of your company's overall network health to review and identify different 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 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 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.

- Is your firewall and antivirus properly configured 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 we can practically guarantee our team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – we just see it all too often in the numerous 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 that 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 will report it to you.

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 do a network review.

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 610.293.0101 or you can e-mail me personally at slorino@paralleledge.com.

Dedicated to serving you,

Sondra Lorino
Web: paralleledge.com
E-mail: slorino@paralleledge.com

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

Deep Expertise and Knowledgeable
"*I've used your services both as an IT manager for a larger firm, and on my own as a sole practitioner. The breadth of your knowledge about the issues facing both large and small businesses is great. I've also made valuable professional contacts, and friends, at PE.*"
– Kathy Dowdell, Principal of Farragut Street Architects

Very Reliable and Responsive
"In a word, reliable. I know I can always count on the PE team to resolve whatever issue we're having in a timely manner. You guys have never left us hanging, whether it's a minor issue or an all-out emergency. We've definitely moved away from the constant break/fix & are focusing on long term projects for improvement. With PE's guidance & recommendations, we've made significant technology strides within the past few years that have set us apart from others in our industry. We're more knowledgeable of what's available to keep us efficient & relevant in an ever evolving technology driven world."
– Colleen Pannulla, Executive Assistant of EDA Contractors

Transparency In Service

"We're delighted with Parallel Edge's service and happy that we made the switch in IT service providers. We are now moving away from putting out fires and paying for nebulous "management," and instead moving toward long-term, specific systemic improvements."

– Dan Gregory, Business Development Manager of CLR Design

Focus On Service, Rather Than Sales

"Parallel Edge Employees do not mess around when it comes to time management. In my experience, IT guys will stand around twiddling thumbs while waiting for a scan or an update to complete. The staff at Parallel Edge will find other tasks without being asked to fill the void and avoid wasted time. Also, I appreciate that there is no continuous up sell of software and peripherals that we simply do not need"

– Justin Moyer Office Manager of Patriot Construction

As A Client We Are Not A Commodity

"Your level of responsiveness is amazing. I never feel like I am just leaving a message when I contact you for help. I feel like everyone in the office is there to help us and you make me feel like I am your most important client every time I talk to anyone at your firm.

It is easy for an IT company to do a good job when things are going well. You can separate the great ones from the also rans when problems pop up. And, on top of troubleshooting and fixing problems the preventive work that you do allows us to know if a problem can be avoided it will be."

– Casey Price, Partner, Price and Price Elder Law

Proactive and Competent

"We have fewer problems and issues that arise because we have a competent person consistently visiting our office. I feel that we are now in a position where we can be more proactive rather than reactive."

– Katie Guzinski, Marketing Director of Marguerite Rodgers, Ltd.

Long Term Collaboration

"*We have been working with Parallel Edge for over 18 years. They have expanded their services to keep pace with our changing needs. We rely on them to keep our IT infrastructure current.*"

– Joan Marchesani, Principal of IEI Group

Understanding Our Specific Needs

"Our previous IT person was a friend who provided IT on the side. *While we were confident in his abilities, it was the responsiveness that we could not rely on. Also, he was just a one-man operation, so there was no depth of knowledge or capabilities. We were limited to his expertise and experience. With Parallel Edge we have IT support that understands our specific needs. Your background and experience in our specific industry was a big selling point for us.*"

– David Pollock, Partner of Building Systems Engineering Group, LLC