

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: TOSS C3
Author: Greg Hanna
www.TOSSc3.com
info@TOSSc3.com
Sales: 1-888-966-9514

Are You a Sitting Duck?

Your company is 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 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...** You! 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 gain's 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 or vendor you trust) is still 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 of 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.

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, 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 IT 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 (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. **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. Employees are now even 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 Wi-Fi.

6. **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 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 even 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.

The Good News for TOSS C3 Clients

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.

As part of our regular security and network auditing for your account, the TOSS C3 team are monitoring a multitude of reports and dashboards to determine:

- Is your network really and truly secured against the most devious cybercriminals?
- Is your data backup TRULY backing up ALL the important files and data you would never want to lose?
- 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?
- Are you accidentally violating any PCI, HIPAA or other data-privacy laws?
- 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?

We know it's natural to want to think, "We've got it covered." **Yet we can practically guarantee that at some point 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 dozens of businesses we've audited over the years.**



About The Company

TOSS C3 has been delivering cloud based technologies and cybersecurity services since 1999, then known as ASP and MSSP. Our Cloud philosophy is, clients are putting their critical IT functions in our hands, therefore we must deliver a superior client experience by guaranteeing speed, reliability, security, and support.

Founded in 1985 as a software development and network implementation company, TOSS C3's ongoing mission is to deliver the fastest and most secure cloud solutions in the industry. What drives our executive team is the constant and never ending fine-tuning to make TOSS C3's cloud as reliable and dependable as a paper and pencil. After all, TOSS C3 is in the IT business and our clients are not, so we merely provide the technological means which allow our clients to focus on their business and be the best in their industry.

Dedicated to serving you,

Greg Hanna
President & CEO
greg.hanna@toss.net

Want to learn more about Cybersecurity? **Get your complimentary signed copy of my #1 Best Selling book, Sitting DUCK.** Just send me an email with your name and address and I'll get the book right to you.

