# 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.**

BeckTek
I.T. Uncomplicated

Provided By:
Scott Beck, President
BeckTek
764 Coverdale Rd.
Riverview, NB  E1B 3L5
www.becktek.ca

# Are You A Sitting Duck?

**You, the CEO of a 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 North American businesses.

**Don't think you're in danger because you're "small" and not a big target like a Staples, Home Depot or Ashley Madison?** Think again. 82,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at smaller 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 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 or Cyber Threat. The impact and costs of such events continue to grow 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 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, 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 without protections in place.

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 Microsoft Windows, Office, 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 technology management service 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, monitored and tested at least monthly; 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 WiFi.

However, should you decide to allow the personal devices, you MUST ensure they are monitored and secured – and a signed policy outlining company data can and will be wiped from the devices should they be lost or the employee leaves the company.

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.

   I highly recommend investing in a managed Universal Threat Management System (UTM). The UTMs are basically firewalls on steroids providing even more protection than a traditional firewall including Intrusion Detection and Prevention, content filtering, web traffic monitoring and more. They are also priced quite competitive compared to a traditional Firewall.

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!)

   So here are 2 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 24-48 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. All of these things will greatly improve the security of your accounts.

## Want Help In 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 **Security And Backup Audit** of your company's overall network health to review and validate as many as 27 different 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. 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 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 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, DPA 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. In Canada, the new Digital Privacy Act contains fines up to $100,000 for companies that fail to take adequate protection against Cyber-Criminals

- 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 or control?

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 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. 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 Security And Backup Audit**. 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 506-383-2895 or you can e-mail me personally at scott@becktek.ca

Dedicated to serving you,

Scott Beck MCSE, Network+, A+

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

**….. productivity has soared……**

"We have worked with several IT providers over the years that promised great things but failed to deliver. BeckTek is the first IT provider that actually backed up their talk with real action. They have exceeded our expectations and continue to impress. Computer frustrations are a thing of the past and our productivity has soared. If you are looking for a true partner to oversee your technology and look after your best interests, BeckTek is the answer."

*Lise Bourque, Director, Brunswick Sheet Metal*

**…no discernable downtime…**

"BeckTek is an important member of our team. Their proactive approach to support keeps our systems running with no discernable downtime and they respond quickly to our questions or if an issue does arise. One would be hard pressed to surpass the quality of service we have received from them. We would highly recommend BeckTek to any business looking for IT support."

*Frederic Gionet, 3+ Corporation*

…**our best interests are being looked after…**

With BeckTek, I know our best interest are being looked after as they ensure we have the best solutions for our needs. Their proactive approach to technology means problems seldom crop up however they get things sorted out quickly and efficiently when they do. BeckTek is a provider I would strongly recommend.

*Nancy Whipp, CEO, CPA New Brunswick (Retired)*

**… productivity has effectively increased…**

"Our experience with BeckTek has been exceptional. Since implementing their proactive approach to IT management, our service requests have dropped by 75% and productivity has effectively increased because we are no longer spending hours troubleshooting and trying to resolve IT issues. Having BeckTek as our trusted Technology Management Firm, I have the peace of mind that our needs are being well looked after."

*Sam Lanctin, Registrar, New Brunswick College of Pharmacists*

**…knows technology…**

"BeckTek knows how important technology is to business having seen the impact on the bottom line when technology goes astray. The preventative measures BeckTek brings to the table are well worth the investment."

*Paul Robichaud, President, EPR Robichaud – Certified Professional Accountants*

**…it all just works…**

"Technology is a part of today's business world. BeckTek understands this and makes having an "IT Department" within reach for any size company. They are very easy to deal with, deliver on their promises and have taking the thinking out of IT for us. Now it all just works and if there is a problem we have the peace of mind knowing they will get it taken care of quickly and efficiently. They have made IT a tool for us, not a drain of resources and time."

*Marc Gallant, CEO, Arbitrium*