CONTINUOUS

WE MAKE IT PERSONAL

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

*This free guide is provided as an educational service by:*

**Jason Silverglate,** Chairman & CEO**, and Ross Brouse,** President & COO **Continuous Networks, LLC. 1 Meadowlands Plaza**

**Suite 200 East Rutherford, NJ 07073**

**Dear Colleague,**

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit."

Look around your office.
How many printers, scanners, copiers, computers, laptops, webcams, tablets, and smartphones do you see?

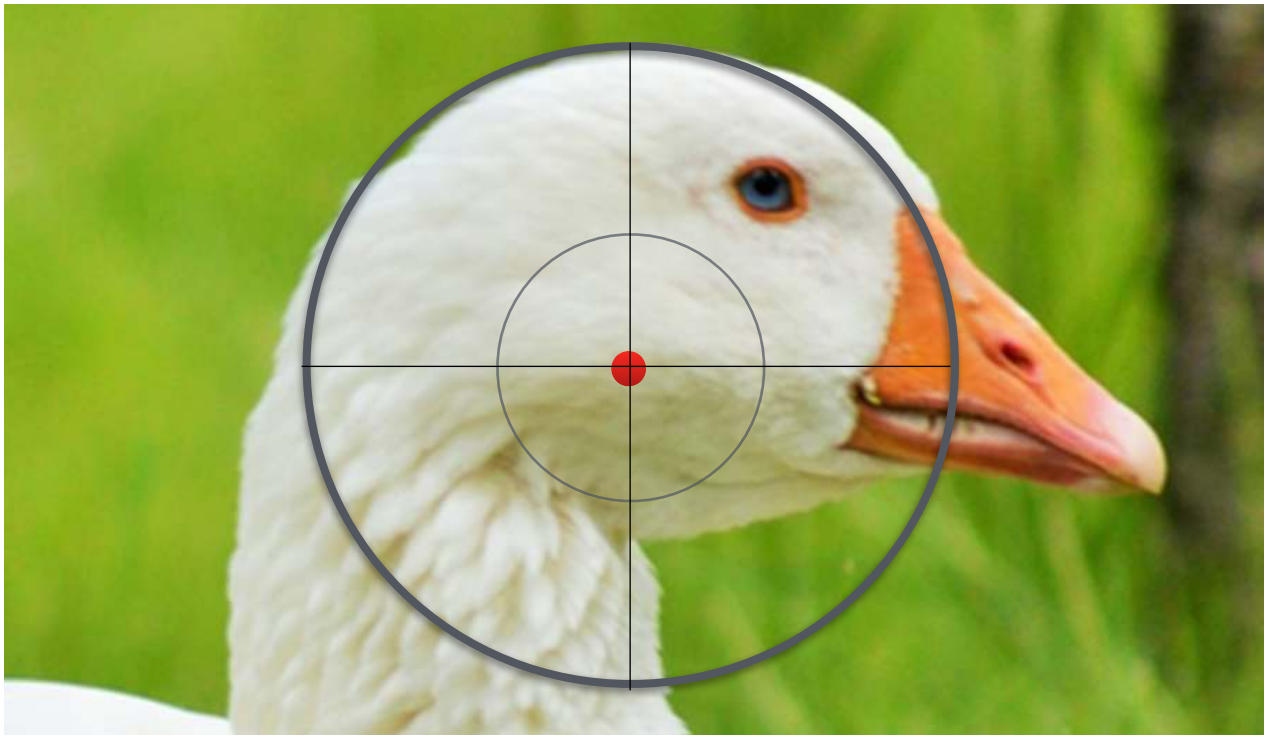
*Every one of them is a ripe target for hackers.*

***Don't be their next victim!***

***IF you want to have any hope of avoiding a cyber-attack, you MUST read this report and act on the information we're providing.***

**Continuously serving you,**

**Jason Silverglate** Chairman & CEO | **Continuous Networks**



## 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 the Ukraine are using sophisticated software systems to hack into thousands of 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 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 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.

   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.

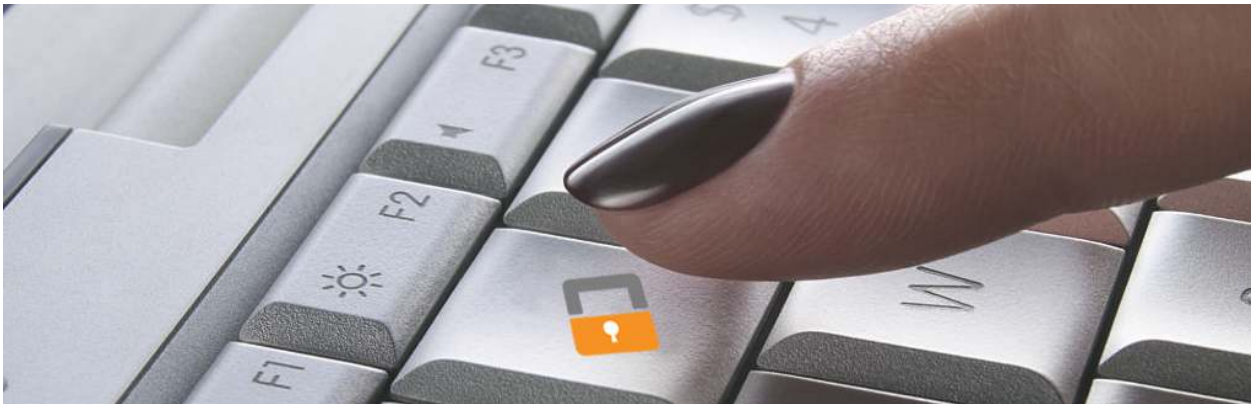

4. **Have An Excellent Backup.** This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee 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.

# 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 to your office to conduct a **Free Security And Backup Audit.** This offer is valid for businesses with 20 or more computers and a minimum of 1 server. We will perform this assessment of your company's overall network health to review and validate as many as 15 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, 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 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 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 **(201) 579-2086** or you can e-mail me at success@continuous.net with subject line "Free Cybersecurity and Backup Audit".

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

**"Continuous Networks is Different"**

I have been an office manager at various companies for five years in New York City. One of the hardest vendors to find has always been the IT vendor. I always felt like I had to apologize to my vendors for submitting help requests; somehow, I was bothering them.

Continuous Networks is different. Help requests are welcomed and quickly managed, both remotely and in person. They think about our IT needs as if they were their own, and they do not stop trying to solve issues until they are solved. They geek out on new technologies, always testing them for themselves before they offer new solutions to us. Even better, they never attempt to sell us solutions that do not work well or that we do not need. Their staff is down- to-earth and personable, and they all feel like members of our own staff. They are our IT directors, and IT has never been smoother than it is now.

—**Steven Eheart** | Human Resources Manager | The Interactive Advertising Bureau

**"The Value, Service, and Peace of Mind is Exemplary"**

I cannot recommend Continuous Networks enough for the service, reliability, and overall peace of mind that they are able to provide my staff. Whenever I send the team questions or support tickets, their response is always immediate and thorough. Continuous has superlative know-how and a customer service mentality. They aren't just a vendor, but a PARTNER. Our company is in a big growth period, and not only does the Continuous team respond to our immediate needs, but they proactively project into the future based on where we're heading. The balance of dealing with current status quo while being able to seamlessly, patiently, and/or quickly move us to our next level is a tall order that Continuous handles with ease and speed. The value Continuous has brought our company is exemplary. Whether it's the day-to- day IT needs, an overhaul of systems and back-end infrastructure, or ad hoc advice, I know we are in good hands. Continuous is an essential part of our security and business continuity; I can't imagine partnering with another IT management company.

**— Chris Staley** | Office Manager | The Interactive Advertising Bureau

**"Outstanding Customer Service Keeps Comodo Online"**

As the Comodo organization continues to grow, the company relies on the infrastructure and IT support of Continuous Networks to ensure the collection and hosting of information is a growth hallenge that is fully supported. The technical service staff of Continuous is able to address any emergency situation for Comodo, and is equally adept at handling rapidly developing situations crucial for bringing new services to market in an expeditious and cost-effective way.

As we consolidated our colocation footprint in the United States, Continuous provided an unparalleled level of flexibility and accommodation, ultimately making the transition flawless. Now that the consolidation is complete, we trust in Continuous's unique blend of robust infrastructure, security controls and outstanding customer service to keep Comodo services online and fully serviced at all times.

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information. With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

**—Ed Giaquinto | Director of Information Technology | Comodo**

**"Success Driven Partnership" "**

"Our partnership with Continuous Networks began with a need for a simple virtual server for a database. From day one, the **Continuous team took the time to understand our business and understand us.** We soon approached them with the need to deploy a cloud-based file sharing platform with 100% uptime and tight security. We work within a global telecom company's New York City office and their internal network security

protocols prohibited access to the platform we wanted to deploy. We needed a firm with extensive networking experience to work with our internal IT team to make this possible. The team from Continuous consulted with each technical team and architected a solution to overcome this roadblock and provide us with exactly what we needed while maintaining the security that our organization demands.

**The Continuous team is always willing to go the extra mile**. Their expertise and focus on our success shows in every interaction we have with them. I can't imagine partnering with anyone else."

**—Rich Simeone | S-One Communications**

CONTINUOUS

WE MAKE IT PERSONAL

**Continuous Networks, LLC.** 1
Meadowlands Plaza, Suite 200

East Rutherford, NJ 07073

**CONTINUOUS.NET**

**201-579-2086**