SUNDOG

7 URGENT SECURITY PROTECTIONS EVERY ORGANIZATION SHOULD HAVE IN PLACE NOW

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium organizations 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: Sundog
230 E. Lincoln Hwy Suite 200
DeKalb, IL 60115
815.991.2400

Author: Cohen Barnes
223 South Winnebago St
Rockford, IL 61102
www.sundogit.com

Are You A Sitting Duck?

Your organization 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 organizations 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 organizations.

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 organizations; 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 organizations have been victims of cybercrime in the last year – and that number is growing rapidly as more organizations utilize cloud computing, 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. **Train Employees on Security Best Practices.** The #1 vulnerability for and organization's network are 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.

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. 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 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 e-mail and data.

   If that employee is checking unregulated, personal e-mail on their own laptop that infects that laptop, 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 that employee's photos, videos, texts, etc. – to ensure YOUR clients' information isn't compromised?

If that employee is checking unregulated, personal e-mail on their own laptop that infects that laptop, 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 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 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 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.

4. **Keep Your Network Up-To-Date.** New vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office; 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 (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!

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.

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 organization.

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 any data-loss and security loopholes we find. We'll also look for common places where security and backup get overlooked, such as mobile devices and laptops. 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 inappropriate sites, 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 configured properly 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 organization is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the hundreds of organizations 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 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 day of your career. Why risk losing it all? Get the facts and be certain your organization, your reputation and your data are protected. Call us at 815.991.2400 or you can e-mail me personally at cohenb@sundogit.com.

Dedicated to serving you,

Cohen Barnes

www.sundogit.com
cohenb@sundogit.com

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

Paul LaLonde
SHRM-CP
Voluntary Action Center

SUNDOG GOES BEYOND JUST FIXING OUR ISSUES

"Having **peace of mind knowing that our systems are protected, our information is protected**, and our organization, as a whole, is protected is how we feel now that we have engaged with Sundog for our IT services. Sundog goes beyond just fixing our issues. The thing I absolutely love about Sundog is that their staff feel like our coworkers. You can't buy that comradery and inclusiveness. **They take the time to get to know our agency, our needs, and our technical abilities.** They truly feel like they're a part of our organization! Sundog is more than just an IT contractor. They are great people with great hearts that want to ensure that your organization succeeds. They take pride in being an extension of our agency. Relationships matter. Sundog makes sure of that."

Tim Suter
CEO
The Suter Company

ONE WORD COMES TO MIND … EXPERTISE

"One word comes to mind when summing up our IT service provided by Sundog. Expertise. As a CEO, I know that we have access to IT expertise with the Sundog team that I don't have on staff. We are in the food business – hiring and maintaining IT expertise on our staff is not our core, and we know we are better off letting Sundog provide this expertise. **They are very responsive, and their staff is extremely friendly to work with.** If there is ever a problem, **they are committed to fixing it.** Sundog is a firm you can trust to give you great service and high value."

Tom Jackowski
Controller
Nehring Electrical Works Co.

AS A MANUFACTURER, WE FOUND SUNDOG TO BE COST COMPETITIVE

"While we just began formally transitioning our IT services to Sundog, it is already apparent they are taking ownership of our network and proactively managing risks. **Their team possesses solid credentials and experience.** They haven't run away from an issue we have experienced yet. The Sundog team displays a desire to learn in situations they have not experienced before and show a passion for helping us take things to the next level. They also look for opportunities to install technology to increase our productivity. As a manufacturer, we are always watching our costs, **and Sundog is cost competitive.** But, while costs are an important factor, it is also important (for me personally) to actually like the people I do business with. I truly enjoy working with the team at Sundog. The combination of these things made it."