# 6 Immediate Security Protections Every Business Should Have

**Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are ill-prepared. Don't be their next victim! This report will get you started in protecting your business.**

Provided by: 7th Dimension
Author: Joshua Holloway
5005 Windplay Dr. #1, El Dorado Hills, CA 95762
(916) 221-0855
7thdi.com

7TH DIMENSION
IT without limits

# 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 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.

**Do you think you're not in danger because you're "small" and not a big target like Equifax or Uber?** 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, 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 6 security measures in place.**

1. **Train Employees On Security Best Practices.** The #1 vulnerability for business networks are the employees using them. It's extremely common for an unaware employee to infect an entire network by opening and clicking a phishing e-mail. Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Employees must be conscientious of what is being plugged in to their computers. Malware can be spread through infected flash drives, external hard drives, and even smartphones.

2. **Keep Clean Machines.** Protect information, computers and networks from cyber-attacks with the latest security software, web browser, and operating system. Managing your updates, patches, anti-virus and anti-malware software helps protect your business from malware and infections. If you are under a managed IT plan, this can all be automated for you so you don't have to worry about missing an important update.

3. **Practice good password management.** Passwords phrases with a strong mix of characters and contain lowercase and uppercase letters, symbols and at least one number are recommended. Do not use the same password for multiple sites. Do not share your password with others, do not write it down, and definitely do not write it on a post-it note attached to your monitor. Have your network administrator manage password complexity and expiration for all users.

4. **Keep Your Firewall Up-to-Date.** Your firewall acts as the frontline defense against hackers as it monitors all incoming and outgoing traffic on your network. Keeping this hardware and software current addresses ever evolving security threats. Firewall maintenance and monitoring should be done by your managed I.T. firm.

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 thief 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. **Limit Employee Access to Data, Information, and Authority to Install Software.** Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs. 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.

## Want Help in Implementing These 6 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 **Network & Security Audit** of your company's overall network health. Our comprehensive audit uses NIST (The National

Institute of Standards and Technology) security requirements to review and validate access control, accountability, configuration management, identification and authentication, maintenance, media protection, system and communications protection, system and information integrity, and risk and security assessment.

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 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.

- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup? Do your employees have authority to use your computers and internet freely?

Realize that you are an attractive target to hackers. Don't ever say "It won't happen to me."

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'll report it to you.

## You Are Under No Obligation to Do or Buy Anything

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**.

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 that your business, your reputation, and your data are protected. Call us at 916-221-0855.

We are dedicated to serving you.

# Here's What a Few of Our Clients Have Said:

## 7th Dimension Disaster Planning Helped 30 Locations

"When evaluating risk, more often than not, companies overlook the obvious. We look at our strengths, weaknesses, opportunities and threats. Of which, natural disaster never seen to be thought of during these evaluations. As Hurricane Harvey approached and a great deal of uncertainty regarding its effect on corporate operations, 7th Dimension stepped in as a critical piece in our disaster planning. Because of their quick support and leadership from Josh Holloway, CEO of 7th Dimension, we were presented with an array of solutions which resulted in uninterrupted operations for our 30+ locations nationwide." – Kelly Carroll, CPP | Director of Finance

## Dimensional Support Made Preventative Maintenance Easy

"7th Dimension has the technical expertise we needed coupled with flexibility in the level of support to fit our needs. They are really responsive, prioritizing important issues that arise and dealing with them quickly and effectively. We have appreciated their preventive maintenance on our network and the ability to troubleshoot new issues as they occur." – El Dorado Hills Fire Department