CIOTECH
Networks | Computers | People

SMALL BUSINESS NETWORK SECURITY RISKS: What You Need to Know

INTRODUCTION

Are you wondering whether you should believe all the hype surrounding cybersecurity these days? Are you questioning whether your business is truly vulnerable and if it is worth the money to research and invest in a network security solution?

First, a **2016 report released by Symantec** found that small businesses are targets of cybercrime 43% of the time. (Another report, the **2016 State of SMB Security** found that as many as 50% of small businesses had already been hit by some form of cybersecurity breach.) If, for some reason, you still do not feel that 50% is a large number, consider that just five years earlier, that number was only 18%.

Cyber criminals are targeting small businesses at an increasing rate because small businesses, often, do not have protective measures in place that make the hacker's "job" more difficult. Small business owners think they can go unnoticed, but cyber criminals are now becoming interested in low hanging fruit, and, sadly, most small businesses are ripe for the picking.

WHAT IS SMALL BUSINESS NETWORK SECURITY?

Network security refers to any action performed with the intention of protecting your network or system's integrity, safeguard its data, or secure its proprietary information. It may also refer to monitoring the network to be made aware of potential threats before they become larger issues with cybersecurity.

For small businesses, network security is more about **identifying vulnerabilities**, applying consistent solutions, securing proprietary data, and safeguarding against employee error through education. Small businesses need not invest in the same expansive in-house solutions that larger companies use. There are per-seat options available that scale more comfortably than what global operations are employing.

Small business network security focuses on creating redundancies, backing up data, and building obstacles that prevent cyber criminals from perceiving you as an easy target. Email and social media are some of the most common vulnerabilities to cyber threats for businesses today. Employees often bring personal devices to work and access your network with a complete disregard to security. Additionally, they are opening emails in a hurry and not fully processing the risks associated with viewing or downloading every attachment or link.

WHY DOES YOUR SMALL BUSINESS NEED NETWORK SECURITY?

Your reputation, clients/customers, financial well-being, and operation are on the line when you do not have network security in place.
If you own the building your business operates from, you don't buy a fire extinguisher and consider yourself protected from fire; just as you cannot install antivirus software on your computer and consider your cybersecurity vulnerabilities fully addressed.

Your business may be considered small based on the number of employees, but your data is likely very important to you, and, without it, your operations would struggle. This alone makes you vulnerable. Add in the financial aspect of what you store - such as social security or banking/credit card information - you are now a target of interest to criminal minds looking to make money through fraud or extortion.

YOUR BUSINESS NEEDS PROTECTION FROM NETWORK SECURITY RISKS FOR THESE REASONS:

- To protect your client data and proprietary information. Both of which have value on the black market.

- Regulatory or ethical reasons. Your patients, clients, or customers have faith in you to safeguard their information. That trust is difficult to restore once it, and their data, has been compromised.

- Because you have employees accessing your network from their own devices or non-secure networks, increasing your vulnerability.

- You can use your network security measures as marketing benefits to potential customers. While it is considered a customer expectation that data will be handled securely, this transparency on behalf of your security may entice prospects to question your competition about theirs.

- You are less vulnerable to legal fallout after a cyber attack if you had security provisions in place ahead of time.

- To set your business apart. In the near future, customers will become more security savvy and begin asking the tough questions about network security. If your business doesn't have the answers, your competition may be called upon to provide them.

You insure your home and your business against unplanned calamities. You need to protect your data as well. It is a cost of doing business in today's virtual environment.

HOW CAN YOU STAY PROTECTED WITH SMALL BUSINESS NETWORK SECURITY?

As we mentioned earlier, network security for small to medium-sized businesses focuses on prevention through implementing challenges to cyber criminals and backing up data. Here is what that means and why it is important.

DATA BACKUPS

We will start with the easiest item first. While it is not difficult, many businesses overlook the importance of performing simple backups of their data. Or worse, they think they are backing up and realize, too late, that it is ineffective against the security threat.

Why it is important: A backup is critical to regaining business functionality after a security breach. While there are different kinds of security issues, a backup saves you from **becoming a victim of ransomware**, or any form of virus that would corrupt your data. It gives you peace of mind that all is not lost.

Backups are also incredibly easy to do and, in most cases, can be automated. However, many businesses confuse a backup with storing information in the cloud. The cloud alone is not a backup. While it technically does “back up” your files, they are still vulnerable. Many businesses have moved from storing files on a single machine to creating a cloud-based repository for the files. They assume that because the cloud company backs up their files, they are protected. This is only partially true.

If your cloud files are accessed through your network, guess what? They are **vulnerable to ransomware**. This common misconception is one of the most disheartening for business owners because they often know the importance of backups and thought they were doing right.

In order to avoid security risks, your backups must be disconnected from the network. Accessible files can be corrupted. You need a backup system that does not allow for direct access.

CHALLENGES TO CYBER CRIMINALS

Creating challenges to cyber criminals makes you a less desirable target.

Why it is important: In your small business, you need to find ways to make it difficult for cyber criminals because that is the exact reason they are targeting your enterprise in the first place. You have more data than an individual but fewer safeguards than a large company. In a Venn diagram of what cyber criminals want, small to medium-sized businesses are in that golden, happy middle ground.

But it doesn’t take much to move your business out of that sweet spot. You simply need to implement challenges. These should include, but are not limited to:

- Running anti-virus, anti-spyware and malware software.

- Using an intrusion protection system.

- Employing a virtual private network (VPN) for employees accessing the network from remote locations such as traveling salespeople or tele commuting employees. Even employees logging on from home in the evenings should be using this level of security.

- Updating security patches and updates on software as soon as they’re available.

- Educating your employees on what to look for in emails and suspicious websites, helping them understand the dangers.

- Creating a password policy for employees and requiring changes be made every 60 days. Consider a two-step authentication process or password security software.

- Ensuring that passwords are not shared by departments and working with HR to remove people from the network as soon as they leave your employ. Change any passwords they may have been aware of. Passwords also have monetary value on the black market. Never assume a past employee (or current one for that matter) wouldn't sell that information if the price was right.

- Using in-house security and a third-party vendor partner to achieve balance and efficiencies.

- Installing a firewall and keeping its software up to date. Taking the time periodically to ensure it's working properly.

- Using encryption software for sensitive data like employee files or financial information.

- Locking down/password protecting your WiFi.

- Changing any existing passwords that came with routers, hardware, or software. Never use the defaults. This should also include removing any test or default pages that may have come with your server.

- Examining your ports of entry on your network. Are they all necessary?

- Removing programs, services, and software you no longer use. Leaving them active just keeps another entry point for hackers open when it needn't be.

Continual monitoring of your network is also extremely important. According to Microsoft's "Advanced Threat Analytics," the average number of days a cyber attacker remains dormant on a network before detection is over 200. Think about how much data your business accrues within that time.

IS SMALL BUSINESS NETWORK SECURITY EXPENSIVE?

Let’s do a quick calculation because it’s this very question (along with just not knowing what to do) that keeps so many small businesses out of investing in network security. The following will help you **understand what a network breach could cost you**:

- Add up your total records of data, any customer or client data that is of value to you. (We won’t even touch prospects in this calculation, although they can be valuable as well.) How many do you have?

- Now multiply that number of records by $154 or $363 if your business is in the healthcare industry. No one said cybersecurity was fair.

- Marvel at how high that number is. Now imagine writing a check for that amount.

According to IBM’s “**The Cost of Data Breach Study**,” $154 is the average cost of a lost or stolen customer record that contained confidential or sensitive information, such as financial details. $363 is the estimated cost of a healthcare record.

DOES A NETWORK SECURITY SOLUTION *STILL* SOUND EXPENSIVE TO YOU?

Let’s add one more qualifier. What is the cost going to be to your brand when your customers, clients, or patients know that you exposed their data? At best, you’ll lose some of them and they will go elsewhere because they do not feel you are **keeping their data secure**.

At worst, you will see them in court. Some people who have experienced stolen data at the hands of a company they do business with, have pursued their options in court under civil action lawsuits. If a company fails to exercise “reasonable care” in protecting their clients’ files and data, and a security breach occurs as a result, those affected by the event may take legal action against the company. **Target Corp.**, for instance, is currently involved in over 140 lawsuits over these exact issues.

If you have no network security in place for your business, you have just made that group’s job of proving “failure to exercise reasonable care” very easy. And if you think cybersecurity is expensive, consider what attorneys charge and what courts award.

WHAT YOU DON'T KNOW ABOUT NETWORK SECURITY CAN HURT YOU

Many small business owners fail to take reasonable precautions because they just don't know what to do. **Is anti-virus software enough? Do you need managed IT services?** There are a lot of questions and many of the answers can bring up even more questions. Even when small business owners perform due diligence and research the topic of network security risks, they often feel overwhelmed and wonder which solutions apply directly to their business.

Cybersecurity is an ongoing need. A system that is perfectly protected one day, can be exposed the next day, due to loopholes in outdated software, external devices accessing an internal network, and new viruses or malware.

A **vulnerability assessment** can help you **understand your risk and isolate issues** with your firewall and networks. This reduces your attack surface and gives you greater peace of mind knowing that your specific issues are addressed.

TAKEAWAYS ON NETWORK SECURITY

EMPLOYEE ERROR

Cyber crime is one of the largest threats to small and medium-sized businesses today. Your business cannot afford the disruption, data loss, loss of reputation, and legal battle that could ensue from not being protected.

Cybersecurity is an ongoing effort because it must be personalized to your business. New threats are created daily, software upgrades expose vulnerabilities, and **employees continue to bring personal devices** to access your network.

Taking the first steps towards increasing your cybersecurity is easy. Educate yourself and your employees on the threats and what to look out for. Prepare backups that are not accessible from the network. Create a strong password process and require changes every 60 days, and have a vulnerability assessment performed by a network security expert so that you understand your business' unique cybersecurity needs.

If you're ready to take the pressure off by trusting your business' cybersecurity to professionals, it's time to call CIO Tech. We'll discuss the needs in protecting your business with managed IT services and how cost effective the solution is.

Contact us today for your free assessment at

813-649-7762

CIOTECH

Networks | Computers | People

www.ciotech.us