CISOVISION | MAKE SECURITY EASY

7 WAYS TO IMPROVE YOUR SMALL BUSINESS CYBERSECURITY

www.cisovision.com

Are You Taking Your Cybersecurity Seriously?

No matter how secure you may be right now, you could always be doing more. Review the best practices below to strengthen your small business cybersecurity.

There are two primary reasons why you need to start taking your business' cybersecurity seriously:

- ✓ **The Threat Is Real**: It's estimated that the global cybercrime industry will cause up to $6 trillion in damages in just a few years. Today, the average phishing attack costs businesses $1.6 million, and the average ransomware payout is $116,000.
- ✓ **You're A Target:** It doesn't matter whether you're a big target for cybercriminals like Capital One, or a small organization - 43% of all breaches involved small businesses in 2019.

When everything is going well, the last thing you want to do is think about what will happen when something goes wrong. It's not necessary to dwell on the potential for a security disaster though — you know that it's a possibility, so let's just leave it at that. What's important about this is that you know to cover your bases.

No need to assume the worst — just plan for it, so you know you're protected. As that old saying goes, "An ounce of prevention is worth a pound of cure". Do what you need to do to "prevent" now, so you don't have to pay for the "cure" later. To start, that means understanding the threats you currently face.

Who Are Cybercriminals (And How Do They Operate?)

Cybercriminals operate all around the globe, trying to steal personal information for sale on the Dark Web, or extort significant amounts of money directly from those whose data and systems they compromise. Additionally, unsuspecting employees and unaware personal users can also pose a threat to their own data security by accidentally clicking the wrong link or downloading an unsafe app.

By definition, a cybercrime is, “an intended illegal act involving the use of computers or other technologies.” Cybercriminals employ a range of methodologies to penetrate their targets’ systems, from phishing to CEO fraud to adware.

All of these schemes involve infecting a user’s or business’ network with dangerous malware. A poorly trained employee can be a key part in this process, clicking a link in a phishing email, or downloading disguised malware off the Internet.

How Do You Know If You Are Secure?

Cybersecurity can be a complicated and scary subject that's often ignored because of those same reasons. Most business owners cannot confidently claim that their business is secure.

Can you?

Some of the questions you should be asking yourself include:

- ✓ Are my computers, servers, laptops and mobile devices secure?
- ✓ Is my network equipment secure? (Including Firewall, ISP modem, switches, and WiFi Access Points)
- ✓ Do I have appropriate Anti-Virus and Anti-Malware software installed on your systems?
- ✓ Are my desktops and servers maintained with regular patches and updates?
- ✓ Are my business' passwords strong enough to prevent cybercriminals from figuring them out?
- ✓ Are my cloud-based assets secure?
- ✓ Are my employees informed about Security Threats and how to protect your clients' data?

7 Best Practices To Improve Small Business Cybersecurity

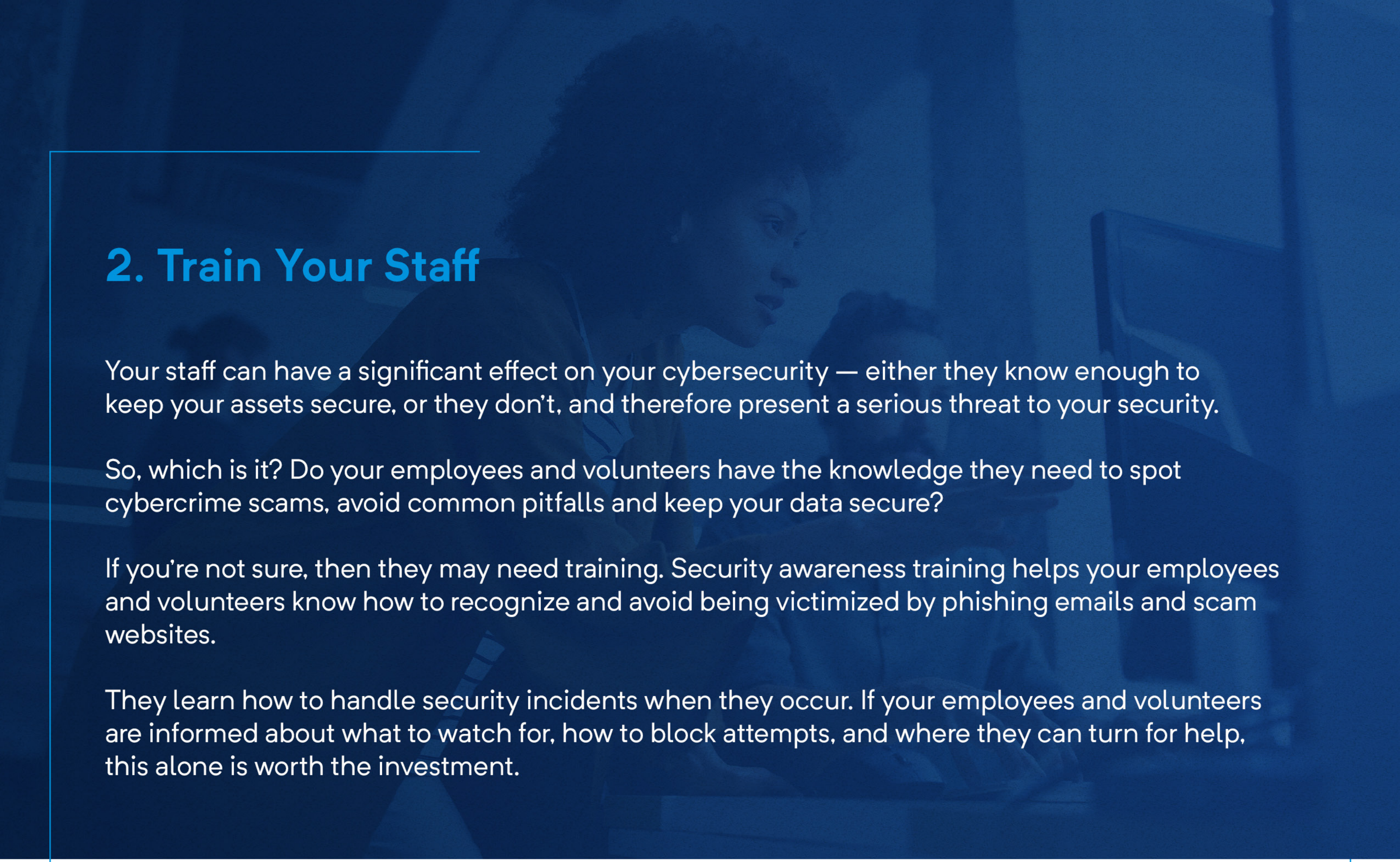
1. Use A Firewall

Your firewall is your first line of defense for keeping your information safe.

A firewall is a particular type of solution that maintains the security of your network. It blocks unauthorized users from gaining access to your data. Firewalls are deployed via hardware, software, or a combination of the two.

A firewall inspects and filters incoming and outgoing data in the following ways:

- ✓ With Packet Filtering that filters incoming and outgoing data and accepts or rejects it depending on your predefined rules.
- ✓ Via an Application Gateway that applies security to applications like Telnet (a software program that can access remote computers and terminals over the Internet, or a TCP/IP computer network) and File Transfer Protocol Servers.
- ✓ By using a Circuit-Level Gateway when a connection such as a Transmission Control Protocol is made, and small pieces called packets are transported.
- ✓ With Proxy Servers: Proxy servers mask your true network address and capture every message that enters or leaves your network.
- ✓ Using Stateful Inspection or Dynamic Packet Filtering to compare a packet's critical data parts. These are compared to a trusted information database to decide if the information is authorized.



2. Train Your Staff

Your staff can have a significant effect on your cybersecurity — either they know enough to keep your assets secure, or they don't, and therefore present a serious threat to your security.

So, which is it? Do your employees and volunteers have the knowledge they need to spot cybercrime scams, avoid common pitfalls and keep your data secure?

If you're not sure, then they may need training. Security awareness training helps your employees and volunteers know how to recognize and avoid being victimized by phishing emails and scam websites.

They learn how to handle security incidents when they occur. If your employees and volunteers are informed about what to watch for, how to block attempts, and where they can turn for help, this alone is worth the investment.

How Do I Train My Employees For Cyber Security?

A comprehensive cybersecurity training program will teach your staff how to handle a range of potential situations:

- ✓ How to identify and address suspicious emails, phishing attempts, social engineering tactics, and more.
- ✓ How to use business technology without exposing data and other assets to external threats by accident.
- ✓ How to respond when you suspect that an attack is occurring or has occurred.

3. Strengthen Your Passwords

Passwords remain a go-to tool for protecting your data, applications, and workstations.

They also remain a common cybersecurity weakness because of the careless way employees go about trying to remember their login information. Weak passwords are easy to compromise, and if that's all that stands between your data in the cloud and in applications, you could be at serious risk for a catastrophic breach.

That's why protecting your login processes with an additional layer of security — multi-factor authentication — is recommended. Multi-factor authentication requires the user to utilize two methods to confirm that they are the rightful account owner. It is an available security feature in many popular applications and software suites.

There are three categories of information that can be used in this process:

- ✓ **Something you have:** Includes a mobile phone, app, or generated code
- ✓ **Something you know:** A family member's name, city of birth, pin, or phrase
- ✓ **Something you are:** Includes fingerprints and facial recognition

4. Protect Mobile Devices

Implement Mobile Device Management and Bring Your Own Device policies that allow employees to use their own devices in combination with the business' without compromising your security:

- ✓ Require password protection and multi-factor authentication for mobile devices.
- ✓ Deploy remote access software that allows you to locate lost/stolen devices, and remotely wipe their data if need be.
- ✓ Develop a whitelist of apps that are approved for business data access.

And don't limit yourself to desktops, laptops, and phones — there's more out there for you to take advantage of.

Have you considered what the Internet of Things and wearable devices can do for workplace efficiency? Now's the time to get on board — up to 20.4 billion IoT devices were brought online last year.

5. Manage Account Lifecycles And Access

This is one of the more basic steps on the list, but no less important. It can't really be automated or outsourced to any technological aids; it's just about doing the work. You need to have a carefully implemented process to track the lifecycle of accounts on your network.

- ✓ Follow a careful system for how accounts are created for new members, how their security is maintained and verified through their life, and how they are removed when no longer needed.
- ✓ Implement secure configuration settings (complex passwords, multi-factor authentication, etc.) for all accounts.
- ✓ Implement controls for login and use, such as lockouts for too many unsuccessful logins, unsuccessful login alerts, and automatic log-off after a period of inactivity

6. Protect Your Wireless Networks

Wi-Fi is a necessary part of doing business. Your staff cannot go without it, so it becomes your responsibility to make sure it's secured, simple as that.

- ✓ Disable the broadcast function so that your SSID is not available for others to see.
- ✓ Use WPA2-Enterprise security, which forces per-user authentication via RADIUS for access.
- ✓ Double-check your radio broadcast levels at default to make sure they don't extend outside your building.
- ✓ Create a Guest Network that's segmented and has a limited bandwidth so that those visiting your building don't have any chance of access to your data.
- ✓ Monitor your network, and log events to track any activity by your employees and other contacts with network access.

7. Limit Unnecessary Physical Access

Your cybersecurity measures won't amount to much if your laptops, tablets, smartphones and other devices are left out in the open for anyone to take.

It's one thing for a cybercriminal to hack into your system remotely. It can be significantly easier if they're doing so directly on a business device.

- ✓ Keep business devices under lock and key when not in use.
- ✓ Maintain a detailed inventory of who has authorized use for specific business devices.
- ✓ Don't leave the login information on a sticky note on the keyboard of the device.

Need Expert Cybersecurity Guidance?

Don't let your cybersecurity suffer, and don't assume you have to handle it all on your own.

CISOVISION is a boutique cybersecurity agency that provides consulting and advisory services to help small businesses like yours mitigate and eliminate cybercrime threats.

You can start improving your cybersecurity in three simple steps:

1. Book a meeting with our team at a time that works for you.
2. Let us assess your cybersecurity and address any vulnerabilities.
3. Get back to focusing on your work, instead of worrying about your cybersecurity.

CISOVISION | RECLAIM YOUR VALUE

www.cisovision.com | (613) 828-1280