THRIVEON
INFORMATION & TECHNOLOGY

Prevent Ransomware

Table of Contents

Introduction

Doing more with less is an imperative for every business to be successful in order to keep costs down, to remain competitive, and because it is not always possible to find enough of the right people to fill positions.

Technology holds the promise of helping you get there but most businesses never obtain it for two reasons.

- 90% of technology approaches are reactive only focused on keeping the day to day running
- IT is thought of as G&A not a functional area so it is treated like an expense and put under finance to be cost controlled

In addition if your IT group isn't doing everything it should to make your company cybersecure, you are inadvertently putting the future of your business at risk.

Learn

What your IT should be doing to help create a secure, predictable platform for you to scale your business more easily and profitably.

- What good managed IT support looks like
- The difference between reactive and proactive IT
- How to implement IT strategy that drives business growth
- How to managed IT to metrics.

Whether your skeptical if your current technology plan can support your business plan, feeling like IT costs too much for what they get, or just wanting to make sure you are not missing something, I wrote this eBook to help you.

Sam Bloedow

Sam Bloedow (Founder and CEO of Thriveon)

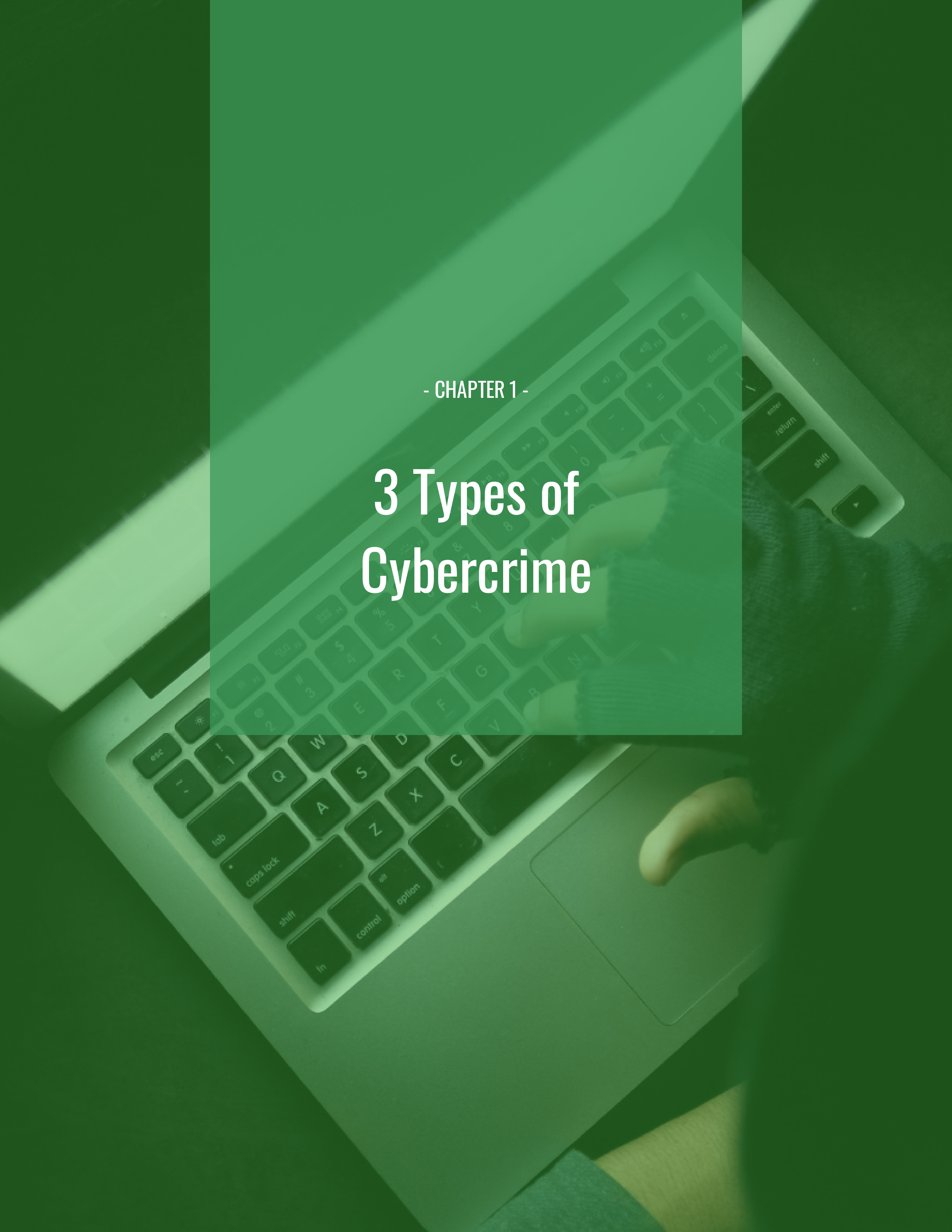
About The Author

Trusting your business can run smoothly with technology seems impossible when your current IT provider is slow to respond and the guidance is reactive. An IT strategy needs to be effective, support growth, and help get your business where it needs to be.

At Thriveon, we believe current IT methods aren't good enough—period. Your managed IT provider should be doing more than just patching issues and managing the day-to-day. They should be proactively preventing issues altogether, before they disrupt your people, and guiding you on the changes to make your business more efficient.

Back in 2005, your struggles were our struggles. We knew we needed a different solution, and so we built one. For the last 15 years, we've deployed an IT approach that supports and guides your business's entire technology spend, including software, hardware, and services so your business can do more with less. We help align your company to best practice standards with a 500-point inspection, reducing security issues and vulnerabilities by 90%, and proactively eliminating risks before they become a problem. It's time for a solid IT strategy to support your business growth and enable you to scale your business the right way.

Sam Bloedow, CEO



- CHAPTER 1 -

3 Types of Cybercrime

3 Types of Cybercrime

If your company is afraid of cybercrime, it's important to understand the bigger picture first. Cybercriminals will infiltrate your system for three reasons:

- To invade your privacy.
- To compromise the trustworthiness of your data.
- To deny access to information.

Once you understand their motives, familiarize yourself with the tactics criminals use to infiltrate your system like phishing, malware, ransomware, identity theft, and scams. To better understand cybercriminals and how to notice, prevent, or fix an attack, we've prepared the following overview. Know how to protect yourself against a costly attacks on your confidentiality, integrity and availability.

Common Types of Cybercrime

1. Confidentiality – Invasion of Privacy

Your company doesn't have to be in health care or financial services to hold data that's considered private or valuable. Cybercriminals will monetize your:

- Employee information
- Customer records
- Contact lists.

They'll extract any valuable data from email addresses to social security numbers. Some of this information can be monetized right away, but often your data is sold to others who compile it with data from other sources. In this way, criminals build a more sophisticated attack.

Intellectual property like designs, drawings, plans, trade secrets, and know-how is a valuable commodity to those who want to attack your competitive edge.

Cyber security and privacy are external and internal concerns. Just as you need to protect information from outsiders, create policies that guide internal access to information in a way that protects your company from harm. We can show you how to protect your data at all access points.

Download our Cybersecurity E-book: Guidelines for Secure Behavior Online and in the Office

2. Integrity – Compromises to the Trustworthiness of Your Data

You don't hear as much about data manipulation crimes as you do with confidentiality but as hackers become better at entering systems, the risk of this type of cybercrime is increasing. The motivation behind an integrity attack can be:

- To compromise decision making.
- Cause damage to the company reputation.
- Commit fraud that will result in monetary gain.

Examples of attacks on data trustworthiness might include:

- Changing the destination for invoice payments or payroll deposits.
- Hijacking communications systems such as email or social media to make unauthorized messages or transactions.
- Modifying data that will change the outcome of a situation.

Entry might occur when an employee uses unsecured methods to access company email and files. Other times someone inadvertently downloads malicious code that opens a door to the intruder. By educating your staff and placing safeguards, you can protect yourself against these type of cyber security breaches.

3. Availability – Denying Access to Your Information

Sometimes hackers will target information in an availability attack and other times their goal is access to a machine or network. Perform a google search for “hospital hacked” and you’ll find a disturbing trend. While hospitals are a big target, the use of ransomware for extortion is not limited to the healthcare field.

By threatening a denial-of-service (DoS), or holding data hostage, a hacker can demand a ransom payment. If you don’t pay, they can disrupt your operations and damage your company’s reputation or ability to do business.

With the increasing number of devices connected to the internet — from smartphones to manufacturing machinery — hackers have an ever-growing list of targets for malware and availability assaults. You might believe you’re immune to attacks but small businesses are easy and frequent targets. We can help your business reduce its vulnerability to availability attacks by protecting thepatchesand ports in your network.

Common Cybercrime Tactics

Now that you know why cybercriminals may be attacking your system , here are some common ways hackers try to obtain your data along with ways to notice, prevent and recover from attacks.

Phishing

Phishing attacks are the most common security breaches. Cybercriminals use email, social media, or other forms of communication to steal data or gain access to networks.

Common email phishing scams embed a link in an email that redirects an employee to a website that asks for sensitive information. We’ve all been warned not to put a password into sites we’ve been directed to via email. But during a hassle-filled day, how many of us remember?

How to Protect Your Business from Phishing Attacks

1. Train employees.
2. Reset passwords.
3. Use spam filters.
4. Increase login security.

Employee training helps with this one. After training, some companies even test employees by using a product that sends fake phishing emails to staff and reports how many were opened. This type of program can help you gauge how effective your training is and help you to refine programs to be more interactive for your staff.

Placing protective measures is also important. Ensure that all passwords are reset regularly and that they're sufficiently complex. Use spam filters to recognize emails from suspicious sources and prevent them from ever reaching employee inboxes.

Deploy a web filter to block malicious websites and encrypt all sensitive company information. You could even disable HTML email messages. Deploy two-factor identification to prevent hackers who might have one form of user credential — such as a password — from gaining access to a website.

Using a proactive IT firm to set up and manage your safeguards can be a huge relief for small businesses that already have enough on their plates.

Malware

Malware is an abbreviation of "malicious software." It refers to software that is specifically designed to gain access to or damage a computer. The term encompasses a broad swatch of cybercrime tactics and types of malware attacks include:

- Spyware
- Viruses
- Worms
- Trojan horses
- Adware
- Botnets

Any of these can infiltrate a computer and send information stored in the company network back to cybercriminals.

How to Prevent Malware Attacks

1. Determine if your machines are already being compromised.
2. Stay on the lookout for future attacks.
3. Protect your systems against malware infiltration.

Educate yourself and be aware of how a malware or botnet will manifest in your environment. For example, you won't see your computers slow down, as infected computers were prone to do in the past. Today's malware knows to do its work on a computer when the computer is idle without calling attention to itself. So, when all is quiet, there could be an issue.

A good way to determine the presence of an attacker is to scan outbound communications records to find communications to suspicious domains. Look at your DNS server to see if you have outbound requests to websites that end in .ru or .cn. Unless you're doing a lot of business with companies in Russia or China, communication with those countries should be investigated. A huge percentage of malware comes from them and frequent communication with sites in those countries is a strong sign your IT equipment may be compromised.

Take action to prevent future attacks by ensuring all your computers on a network aren't running the same operating system. Reinforce to employees the importance of staying away from suspicious websites and not clicking on email attachments. An IT service provider can assist with all of these efforts and help monitor your network for signs of potential malware.

Ransomware

Ransomware, often spread through email attachments, is a type of malware. But unlike malware, which self-destructs or flies under a company's radar, ransomware attacks will alert users that their data has been compromised. What's the logic? As the name implies, ransomware creators profit by holding your data hostage. The attacks can lock devices and render them useless until you make an online payment. Or they lock you out of your data until you pay the ransom specified by the attacker in return for access to your own data.

How to Prevent Ransomware Attacks

1. Establish best practices.
2. Update antivirus software.
3. Install software patches.

Protect yourself by establishing best practices that all users to follow. Be sure employees are properly trained on malware prevention. This includes not opening suspicious emails or clicking on links within emails. Inform your users that documents seemingly not directly related to the web, such as PDF documents that contain live links or Javascript can link to botnets or malware.

You'll also want to regularly update your antivirus software. Not too long ago, people updated their antivirus software once a month. Now, it should be at least hourly, but bigger firms often update constantly because things develop that quickly.

And don't forgo the endless routine of installing software patches to mend holes through which botnets and malware could slip. If you're unsure where to start or feel overwhelmed, a proactive IT provider can enact practices to keep ransomware from impacting your business.

Identity theft

Identity theft is a well-known cybercrime tactic, but employees can still find themselves vulnerable. This, in turn, makes their employers vulnerable, as well. Identity thieves gain access to an employee's personal information and use it to their own ends.

How to Protect Your Business from Identity Theft

1. Train employees.
2. Reset passwords.
3. Filter email

Many of the practices used to combat phishing attacks work here, too, because phishing is the ultimate form of online identity theft.

Cybercriminals can send emails that seem as though they're from an employee's colleague or business contact. Ensure employees never email personal or financial information, even when they know the recipient. Employees should never give any type of business information via the internet whether on a website or by email.

Scams

Scams are carried out through email, social media, and mobile apps. On social media, scammers pose as people's friends or make up profiles, gain trust, and ask for pertinent business or personal information.

Consider placing all social media sites behind a firewall. This can be hard to do if employees need access to certain social media sites, like LinkedIn, for work.

How to Protect Your Business from Online Scams

1. Educate employees on existing scams.
2. Never email sensitive information.
3. Send weekly reminders.

Ensure employees are familiar with the latest scams. Some of them appear to be from social media sites like Facebook or Twitter and claim an employee's account has been closed or canceled. The email provides a link to click on to reinstate the account. Clicking on the link gives cybercriminals enough information to hack into accounts or can install malware onto a computer.

Another scam seems to be from executives or another employee in your company and asks for sensitive information like W-2 or wage statements. If the person receiving the email thinks it's real, the cybercriminal gains access to employees' personal information and your business information.

Other scams look like emails from shippers and claim to offer tracking information for a package sent to an employee. Click on the link in an email and a virus is loaded onto the computer, smartphone, or tablet the employee has used to access email. Such a virus can capture every keystroke to get username, password, and sensitive business information.

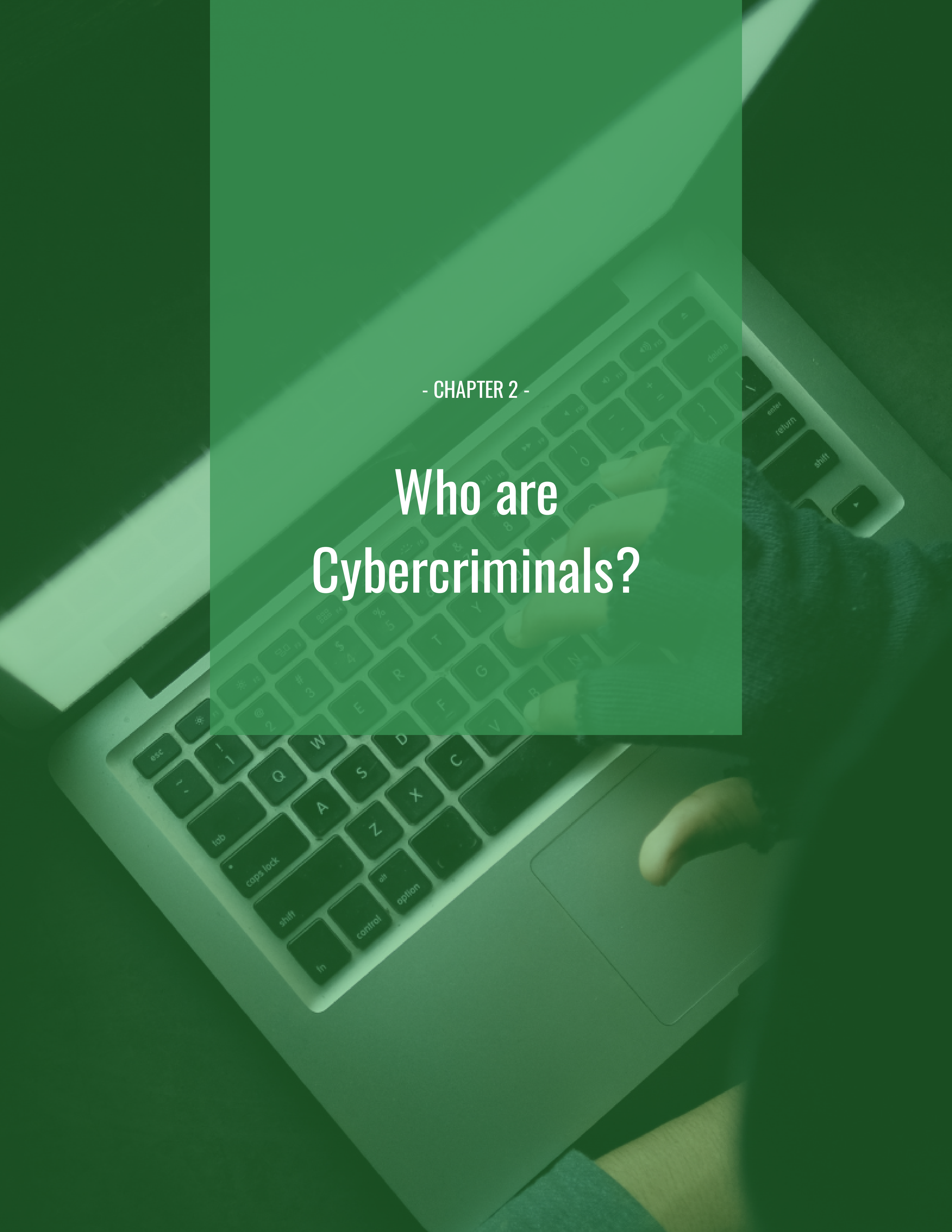
The scams may change but the takeaway is simple. You can appraise employees of current scams, but the bottom line is they shouldn't click on any link or open an attachment in an email they weren't expecting. You may need to send out weekly reminders.

Cybersecurity is Our Business

Assess your risk for cybercrime. Consider the information that you use and store in your business. What damage would you suffer if you were the victim of a confidentiality, integrity, or availability cyber attack.

Undoubtedly, security is not just an IT concern. It's a business concern. The reason why many companies fall behind in this area is that they lack expertise.

Managed IT Service Providers, like Thriveon, partner with companies to supply the cybersecurity expertise and technology tools that thwart the growing threat of cybercrime. We can take the burden and fear of cybercrime off your company with a customized IT strategy that is aligned with business goals.



- CHAPTER 2 -

Who are Cybercriminals?

Who are Cybercriminals?

Cybercrime is a $6 trillion industry and growing. It’s six times larger than the drug trade and would count as the third largest economy in the world behind the U.S. and China. By 2025, cybercrime is projected to be a $10.5 trillion industry. We don’t often see the faces of cybercriminals, so... who exactly are they?

Organized crime gangs account for 55% of cybercrime. They operate on the dark web – an underground marketplace for digital information that can be used to extract payment. While Russia and China tend to get the most attention, 26% of active cybercriminals are from North America and 17% are from the European Union. Let’s look at who they are and why cybercrime continues to grow and affect so many businesses.

Why Cybercrime is Growing

The pandemic shifted the way people do business. Suddenly everyone was working online and remotely. In the rush to accommodate this shift, companies opened a lot of new vulnerabilities. More and more people had to rely on technology and existing precautions while the landscape was drastically changing.

During the pandemic, hacked companies paid an average of $21,659 for a cyberattack. Nearly 85% of these attacks were successful because they defrauded humans vs exploiting technological gaps. In fact, Forbes listed targeting people as the #1 reason cybercrime is increasing. Clearly, companies need to better educate their employees on who cybercriminals are and how they operate.

Cybercriminals are becoming better at doing the research necessary to be successful. They can play the odds with thousands of emails, waiting for you to open the right one. They can operate from anywhere and they can buy information on the dark web to increase their chances of success.

Watch now: The Business Leader's Role in Cybersecurity for the Modern Workplace

What are Cybercriminals?

Cybercriminals are hackers with malicious intent. These individuals, also known as bad actors, crackers, stalkers or pirates, use the internet to access data and files that they can use for their own gain.

The motivations of cybercriminals can vary. A lone cybercriminal might be a disgruntled employee seeking revenge. Highly organized criminal syndicates or political groups may try to sew chaos or extort large amounts of money. No matter how advanced, their motives will likely be one of the following:

- Money through theft or extortion
- Power or influence
- Financial information
- Personal or corporate data
- New product information
- Access to systems
- Adware or spyware placement

It can be difficult to identify and track cybercriminals. Savvy hackers create proxies and anonymous networks to conceal their identities. We can best trace them via their motivations.

7 Categories of Cybercriminals:

Different types of cybercriminals operate in different ways. Here are seven categories of cybercriminal that cover most methods cybercriminals use:

1. **Hackers.** This broad category includes anyone with the necessary technical skill. While most hackers are black hat – using their skills for their own gain – white hat hackers simply enjoy the challenge of hacking without the malicious intent behind it.

2. **Organized hackers.** These groups include organized criminals, political groups, terrorists, and "hacktivists." They're often well-funded and prepared.

3. **Internet stalkers.** These hackers monitor web activity of their victims. They use social media and malware to gain sensitive or personal information.
4. **Identity thieves.** Criminals that use personal info for their gain. Identity theft has evolved from individual theft to the theft of large databases criminals can either sell or use.
5. **Phishing scammers.** Phishing, as the name implies, uses fake emails or websites to lure users to volunteer information like passwords. An unknowing user simply opening an email or link could give hackers access to their network.
6. **Cyberterrorists.** Politically motivated groups that use cybercrime to advance their cause.
7. **State actors.** Hackers that are sponsored by their government to commit cybercrimes. Russia's "Fancy Bear" is one of the better-known state actors groups.

Who do Cybercriminals target?

Unfortunately, cybercriminals will target anyone and everyone. Even small businesses are targets as cybercriminals learn how to leverage any type of sensitive information for their gain. Don't let hackers target your network. We can help you! Keep your business fortified against cyberattack with proactive IT services that anticipate attacks long before they happen. Schedule your free IT Strategy Session to get and stay protected.

Sources: idagent.com, cbsnews.com, forbes.com, online.norwich.edu, blog.avast.com, sciencedirect.com, kaspersky.com, makeuseof.com.

- CHAPTER 3 -

Prevent Ransomware with Complex Passwords and Multifactor Authentication

Prevent Ransomware with Complex Passwords and Multifactor Authentication

"Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."

Avoiding attacks and prevention of ransomware is a top concern for Managed IT services, including here at Thriveon. You can help prevent ransomware by ensuring you and your employees use complex passwords and multi-factor authentication for all logins on company provided devices. These simple prevention measures could mean the difference between staving off or succumbing to a ransomware attack.

Read eBook: How cybersecure is your business?

Prevent Ransomware with Complex Passwords

Make certain that your employees do what you can to avoid a ransomware attack in the first place. By using complex and different passwords for all logins, it's one small way that you can make it harder for a cybercriminal to attempt an attack. Password Managers are especially helpful in helping you store your passwords securely and even provide the option of creating random complex passwords for you, so they are complex, smart, safe – but you do not have to write them down elsewhere or memorize them.

Complex passwords considerations:

- At minimum 12 characters
- Current recommendations are 19 characters
- Consider using a pass phrase
- Use different passwords for each account
- Change passwords frequently

Prevent Ransomware with Multifactor Authentication

Another way you can set up your logins and devices to be more protected is through implementing multifactor authentication. What this means is that for every new login attempt, it pushes a code or prompt to another device that you have access to, so you can verify that it is really you who is logging in. By enforcing multifactor authentication, bad actors need more than your password to access your information.

Creating complex passwords and using multifactor authentication for your logins are just two ways that you can work to avoid ransomware. Let us help to secure your accounts and ensure you are set up to help prevent ransomware. Schedule a meeting today!

*Source:FBI.gov

- CHAPTER 4 -

Prevent Ransomware with Proper Patching

Prevent Ransomware with Proper Patching

Ransomware is a growing issue that costs companies billions of dollars annually. Hackers create encrypted malware that enters your networks, hardware or software and blocks your access until ransom is paid. Usually, you have 24-48 hours to comply. Stopping ransomware requires an aggressive and proactive IT strategy that includes proper patching.

Proper patching involves tracking, testing and documenting your patch updates within a comprehensive inventory of your networks, devices, software and operating systems. Once a patch is applied, it requires testing and monitoring to ensure it accomplishes its intended goal. Why is this process so important? We'll uncover how patching works and why it can affect your security and productivity negatively if not performed regularly within a comprehensive strategy.

Watch webinar: The Business Leader's Guide to Cybersecurity

What is a Software Patch?

Patching is the term for regular software updates and fixes. When you receive a notification on your phone or computer that a software upgrade is available, that's a patch.

A patch at its simplest is a piece of code that the software company develops to add new features, fix bugs or improve security in their product. By adding software updates and patches, you ideally upgrade your software to the newest and best version. But what if it isn't the best? You need to test that each patch is functioning the way you want.

The Need for Patch Management Software

Protecting your business from ransomware attacks should include a comprehensive patch management program. Having a program that tests and tracks your patches allows you to regularly:

- Optimize your software and IT systems
- Fix bugs
- Keep your networks secure
- Comply with security regulations
- Repair vulnerabilities

Without performing regular scheduled patching, you leave yourself open to the increasing likelihood of malware and ransomware attacks.

How to Implement a Software Patching Program

To make sure that you're adding and tracking the right patches to keep your IT systems healthy and productive, follow these six software patching best practices:

1. **Have a cohesive management policy**. Make sure your team has a concise plan on how to keep your IT systems updated with good cyber hygiene.

2. **Scan regularly.** Scan your networks and devices to stay on top of what areas are vulnerable and which patches need to be added.

3. **Test your patches.** Managing patches isn't merely upgrading to the latest version. It means tracking and testing patches once they've been implemented to ensure that they are working correctly. Problems can unexpectedly arise from software patches that don't configure or perform their intended resolution.

4. **Apply patches laterally**. Once a patch has been fully vetted, apply it across your entire system. Don't let sections of your network lapse behind because they weren't properly updated.
5. **Keep detailed reports.** A record of your patching history is invaluable when troubleshooting issues later.
6. **Have a recovery plan.** Always have a backup. If you encounter a glitch because of patching, have a plan in place for how to recover. It could save you countless hours and dollars.

The Advantage of Proactive IT Services for Your Patching

Patching is a complex and evolving process that demands constant attention. It's essentially a full-time job. Using an experienced IT service to carefully manage your patches ensures that a patching expert will always:

- Track *all* your devices.
- Properly manage your firewall.
- Schedule routine checks.
- Test patches.
- Review your patching report.
- Have a recovery plan.

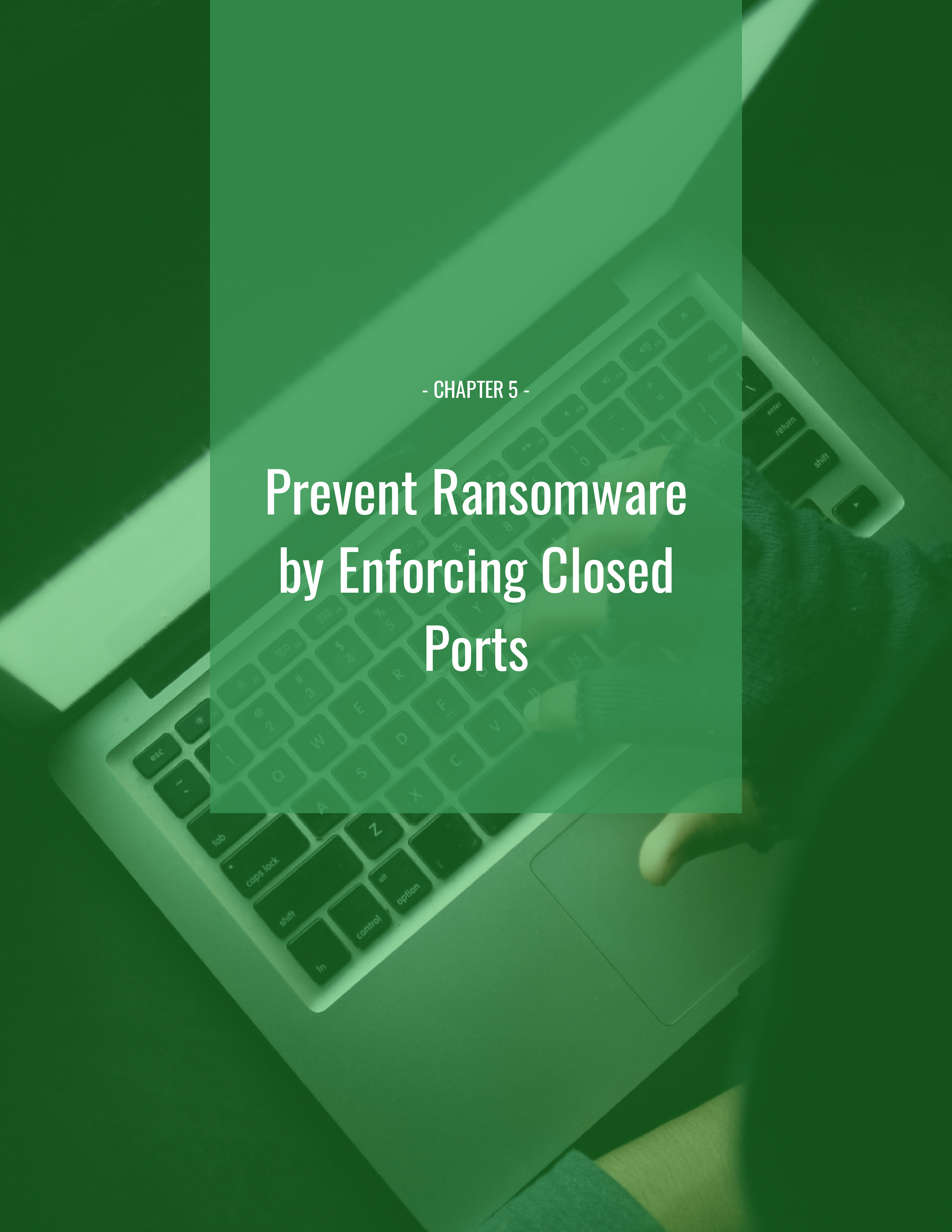
An experienced IT services company like Thriveon will not only manage your patching program, but we'll also proactively act to make sure that your company is ahead of any ransomware risk.

If you don't have the inhouse resources for a 40hr/week patching program, consider the value of a full services IT company. While you could periodically outsource the work, you'd only succeed in resolving patch issues within a small window and without follow up testing. You still remain vulnerable.

Proactive Patch Management for Your Business

Effectively managing, testing and documenting software patches for your business takes time and resources away from your day-to-day operation. Trust this critical task to an IT provider who will proactively manage all your patch updates.

Thriveon will ensure you're never vulnerable and that your productivity doesn't suffer from compromised hardware or networks. Contact us today to learn more about how we manage your technology with holistic patching services.



- CHAPTER 5 -

Prevent Ransomware by Enforcing Closed Ports

Prevent Ransomware by Enforcing Closed Ports

If you left your windows open and door unlocked, you might not be totally surprised if someone broke into your home. The same analogy holds for your business' cybersecurity. When you leave ports between your internal network and your firewall open, you shouldn't be surprised when thieves access your valuable data and inflict costly ransomware.

To keep your business safe from these types of cyberattacks, you need to closely monitor the ports you use. By regularly evaluating which ports are open, which ports you use, and which ports should be closed, you tighten your security and lessen your vulnerability attack. Keep your business firewall secure by implementing a port protection plan.

Watch webinar: The Business Leader's Role in Cybersecurity for the Modern Workplace

What is A Firewall?

A firewall is a security barrier between the internet and your private network. It protects your network's software and hardware from unauthorized outside access and attack. A firewall operates on preset rules and will block out "packets" of malicious data trying to enter. Once data enters your network, an effective firewall can further filter it to ensure your safety.

There are different types of firewalls - either via software or hardware - that offer varying degrees of security:

- **Packet filtering firewalls** are the most basic firewalls but still effective. They check the source IP against the destination IP, like a conductor checking your train ticket. They are limited in that they don't examine the actual data being transferred.
- **Circuit level gateways** perform similarly in that they conduct a single check but with a greater level of security. A circuit level gateway acts as an intermediary that handles the data transfer and keeps the destination hidden from the sender.
- **Stateful inspection** is a higher-level firewall that examines packets more thoroughly. Like a bouncer, a stateful inspection firewall checks the source and destination, the connection and the state of the packets being transferred before allowing them to go through.
- **Proxy server** firewalls offer the highest level of security against internet attack. They create a "proxy" firewall that accepts and examines packets before allowing them into your internal network. A proxy server is like a customs officer that carefully examines data before letting it pass through your gate.

What Are Firewall Ports?

Your business doesn't exist in a firewall protected vacuum. To access the internet, exchange data and conduct business you need "ports" between your internal network and the outside world. The way you achieve this is by opening ports through your firewall.

Firewall ports are necessary but if not effectively monitored and managed, they can become vulnerable to outside malware. No matter what type of firewall your business uses, you'll need a program in place to inventory the ports going through it. The ports you use need to be constantly monitored so that ransomware and other threats don't get. Your program also needs to monitor and close unused ports before they can become a liability.

How to Protect Your Business Firewall Ports

Well-managed firewall settings need to be reviewed monthly. Unfortunately, many businesses don't have the time or resources for a regular port management program. Others simply overlook this important task.

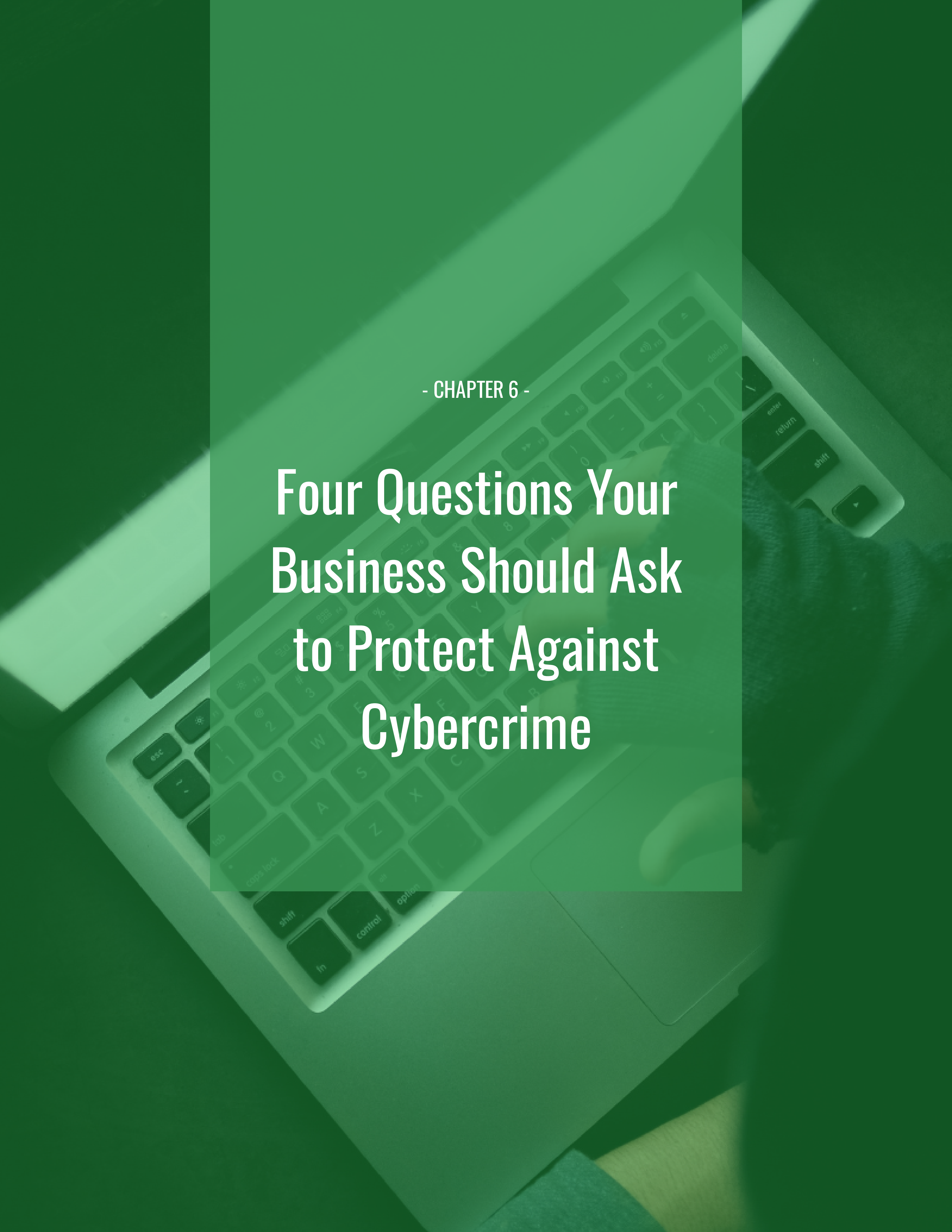
A proactive IT firm can monitor your ports to ensure that your firewall isn't breached via an unused opening. Good cyber-hygiene requires diligence and a system of regular checks to prevent cyberattacks and ransomware from entering through your ports.

An IT firm will also track current cyberthreats to proactively secure your business against them. They can close non-essential ports and secure those you do use. Only the IP addresses you authorize will be allowed. Without an inhouse IT specialist, it can be difficult to achieve this level of protection

An IT expert can also segment your LAN (land area network) so that if malware does enter your system, it can be easily contained without corrupting your entire network. They can also set up an IPS (intrusion protection system) that examines network traffic, identifies vulnerabilities and records threats.

Enforce Your Closed Ports

Firewalls require a diligent administrator to properly install and monitor them. To ensure that your business has a strong and effective firewall without vulnerable ports, contact Thriveon to assess your network today. We provide airtight cybersecurity and business firewall support for Minnesota businesses across the state.



- CHAPTER 6 -

Four Questions Your Business Should Ask to Protect Against Cybercrime

Four Questions to Ask

What would happen if a cyberattack hit your business? When you consider the possibility, it quickly becomes clear that you need to include cybersecurity in your risk management plan. Hackers no longer just prey on large corporations. It's unfortunately very easy for a would-be hacker to get the tools they need to profit from companies like yours.

The cost of cybercrime in the U.S. continues to skyrocket. No one is safe and your business should be protected against the very real possibility of an attack. Here are four questions to help you envision the impact cybercrime would have on your business and what your company can do to mitigate the risks.

1. Will your business continue to operate after a cyberattack?

If you don't want to be in the 60% of small and medium-sized companies that go out of business within six months of a breach, think about what your response will be when your data has been stolen, kidnapped or vandalized.

How you regain control of your digital assets will depend largely upon the type of breach you experience. First, you'll need to focus on how to stop the cyberattack. With your systems down, what will your people do if they cannot work or communicate with customers? Do you have another way to get to the key information you need to complete your daily transactions?

A business continuity plan that details how you use your backups to get up and running again can save you from this paralysis. Have your people practice so they know how to work with a backup before a real emergency occurs.

2. How would a hacking incident affect people?

At the very minimum, a cyberattack will be stressful for everyone. Depending upon what happens, concern could grow. As you work to stop the incident and return operations to normal, everyone will be under pressure to meet customer needs. They might also start worrying about their paychecks, or the survivability of the company. If your HR records were compromised, identity theft may become a concern too.

Then there's your reputation. Will people want to work for you or with you in the future? Will employees and customers stay on after the incident?

The good reputation you have with your customers could be scarred. If you have product designs or any intellectual property that belongs to them, they are going to worry about the future security of their own company. Will there be another attack that will affect them because of their relationship with you? Current cybercrime issues become future cybercrime issues.

New customers will be harder to get if you have a reputation for being vulnerable to a cyberattack. How can you be trusted? Are you even going to be in business long enough to fulfill their orders?

Watch our on-demand webinar to learn how you can better protect your business from falling victim to a cyber attack.

3. What are the legal or regulatory ramifications of a cyberattack?

The data you gather and store has value to your business, your employees, your vendors, and certainly your customers. Depending upon how upset and fearful people are, you could get sued by the people who are involved. The client whose intellectual property was stolen could take legal action because loss of their proprietary information means a loss of their competitive edge.

If your industry has strict regulatory compliance laws such as ITAR, HIPAA or PCI, then you will face fines. You'll come under intense scrutiny as your company, people and policies are studied to see if you failed to implement important protection measures against the breach.

The chances of prosecuting and convicting the real perpetrator are slim. Bad actors (slang for cybercriminals) can be very difficult to trace. The cybercriminal marketplace allows people to buy and sell services woven together in a complex web of interactions that result in yours and other crimes.

4. What are the financial repercussions of a cyberattack?

You can put a dollar sign beside just about every effect discussed so far. A cyberattack is costly if not devastating. You will spend money to deal with the incident and to get operations going again including:

- Legal representation.
- Settlements.
- Loss of customers.
- Inability to attract new customers.
- Loss of employees.
- Protection for those affected by the beach.

Then comes the question: What are you going to do differently so that it doesn't happen again?
Investing in quality IT support that prevents cybercrime will always be less expensive than an attack. The cost of good cybersecurity is nothing compared to the emotional and financial toll a cybercrime can take.

Protect Yourself from Cybercrime

Ask yourself the above questions. How would you respond to a potential cyberattack?

This doesn't need to be a depressing exercise. Use your answers to start a productive discussion about how you can strengthen risk management strategy and cybersecurity at your company. Include technical and non-technical components to both avoid hacking incidents and to improve your ability to bounce back if your company ever does become a victim.

Wondering where to start? Thriveon can help. Schedule a meeting today to get your important questions answered. We know how to protect against cyberattack and we help businesses like yours every day.

- CHAPTER 7 -

Cybersecurity Checklist: Ensure Your Employee and Customer Data is Safe

Cybersecurity Checklist: Ensure Your Employee and Customer Data is Safe

With ongoing attacks and unstable political and social environments, now is the time to be certain your business is safeguarded from malicious cyber-attacks. As a business leader, it is undoubtedly critical for you to take the necessary steps to keep your business safe. 60% of businesses go out of business within 6 months of a cyber-attack. Don't let this happen to you.

Download Infographic: Cybersecurity Checklist

Read the cybersecurity checklist and schedule an introductory meeting to start the conversation on getting your security strategies in place.

Cybersecurity Checklist:

- Get cyber Insurance to financially recover from an attack
- Implement ongoing security awareness and phishing training for you and your employees
- Keep antimalware, computer operating system, and firewalls up to date
- Be suspicious of odd emails and check the spelling of email addresses by hovering your mouse over it
- Be suspicious of links and attachments in emails. Check the spelling of links by hovering your mouse over it. Do not click on or open suspicious attachments.

- Get click protection for your email systems, so if you do click on a bad link, it is less likely to hijack your computer.
- Do not click on ads on a webpage or news site. Ads on these sites can be made to look legitimate, but instead download malware
- Be careful what you post on social media and other publicly facing sites: address, email address, phone number, mother's maiden name, pet's name, birthdate, birthplace, bank account details
- Set unique complex passwords for every login. Easily track this by using a Password Keeper so you only need to remember one password
- Do not save store passwords on your web browser or computer, other than in password keeper
- Do not keep a company list of passwords.
- Do not use public WI-FI. Hackers can set up a look-alike public WI-FI that can read all the information your computer sends through it, including keyboard strokes
- Do not use public computers. They could record your every key stroke
- Call to verify ACH payment requests the first time or if changes
- Turn on two factor authentication to access your company's network and all web portals. That way bad actors need more than your password to access any information
- Enforce a complex password policy. The length of time it takes to crack a password grows exponentially with each character added. 9 characters can be cracked in 2 minutes, 10 characters in 2 hours, 11 characters in 6 days and so on
- Remove users' local admin rights on their computers. By removing local admin rights, the risks from clicking on bad links in websites or emails is reduced because the corresponding action of downloading and executing a malicious payload is less likely to be successful.
- Isolate your backups and backup appliance from your network. When a cyber-attack happens, it is designed to run across the entire network in your business. By preventing your network from accessing your backups and backup appliance you protect yourself, in the event of an attack because you still have secured data to restore.

This is just the beginning

These cybersecurity basics are just the first steps to getting you and your team cyber-aware and cybersecure. Schedule an introductory meeting today to learn how we guide and implement IT best practices for your business' highest safety and security.

Download Infographic: Cybersecurity Checklist

THRIVEON
INFORMATION & TECHNOLOGY

Schedule a Consultation

Learn more about the benefit's our proactive approach would have in your business.

Schedule a Consultation