THRIVEON
INFORMATION & TECHNOLOGY

How cybersecure is your business?

Table of Contents

1. Introduction

2. About The Author

3. Types of Cybercrime

4. Security Awareness for Your Business

5. The Importance of Cyber Resilience

6. Is Your Company's Online Data Secure?

7. Optimizing Your Business's Cybersecurity

8. Quick Guide to Cybersecurity

9. Helpful Security Hints

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.

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

Sam Bloedow, CEO of Thriveon

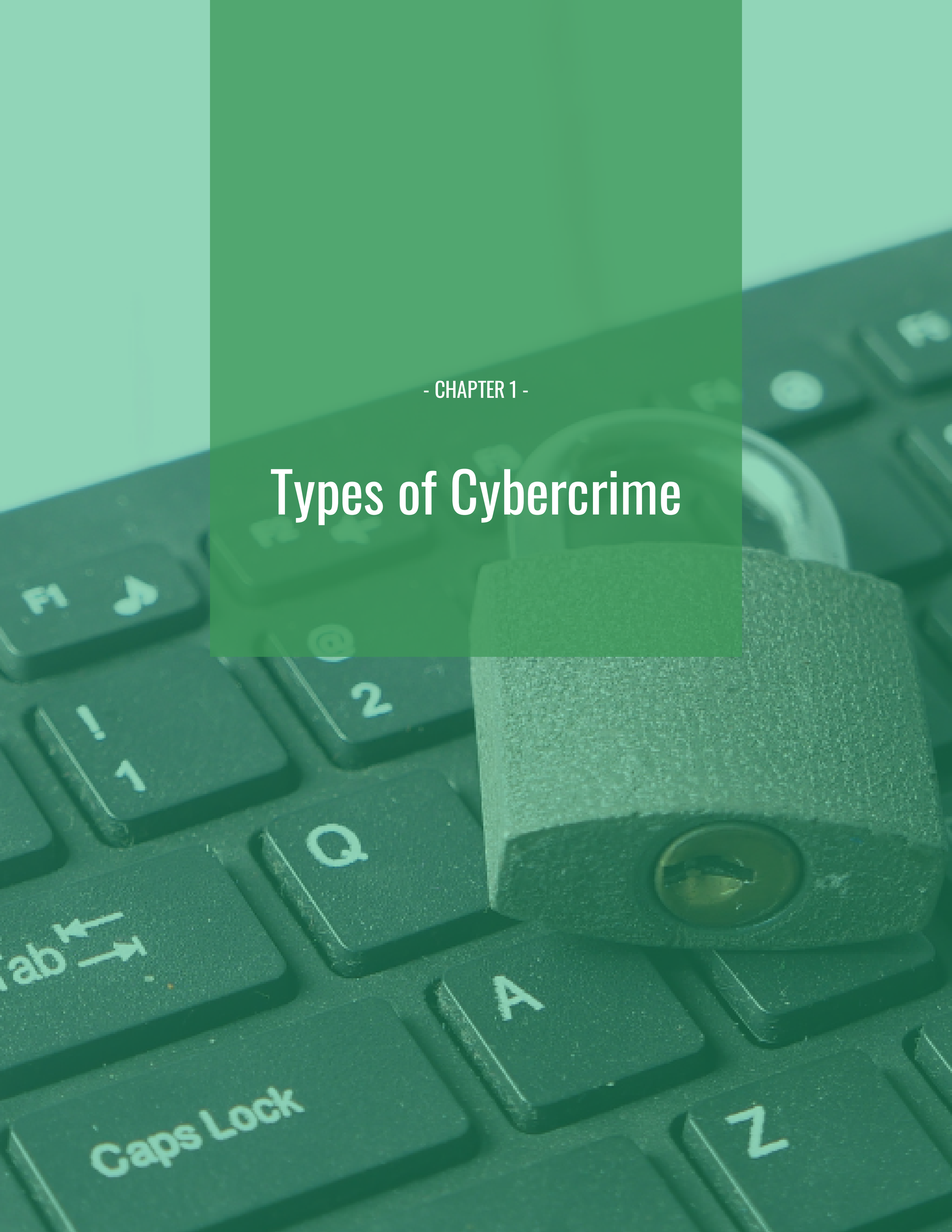
Trusting your business can run smoothly with technology seems impossible when your current IT provider is slow to respond and the guidance is reactive. An IT strategy needs to be effective, support growth, and help get your business where it needs to be.

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.

- CHAPTER 1 -

Types of Cybercrime

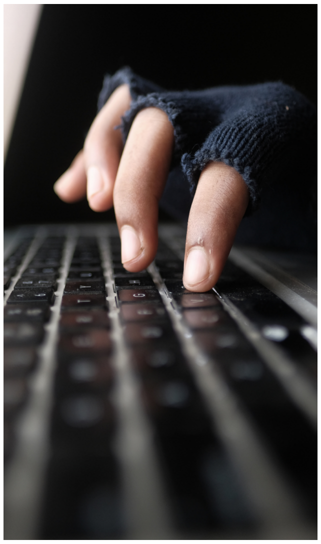


Types of Cybercrime

If you're a company executive afraid of cybercrime, it's important to understand the bigger picture first. Cybercriminals infiltrate your system as a way to invade your privacy, compromise the trustworthiness of your data, or deny access to information. Once you understand that, it's smart to familiarize yourself with the tactics these criminals use in order to infiltrate your system such as phishing, malware, ransomware, identity theft, and scams.

Here's what you need to know to better understand cybercriminals and how to notice, prevent, or fix an attack.

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 should be considered private. Cybercriminals want to monetize your employee information, customer records, and contact lists; from email addresses to social security numbers.

Some of the information that is stolen can be monetized right away, but often it is sold to others who compile it with data from other sources to build a more sophisticated attack. Intellectual property in the form of designs, drawings, plans, trade secrets, and know-how is valuable to those who want to attack your competitive edge.

Privacy is an external and internal concern. Just as you need to protect information from outsiders, policies that guide internal access to information can also protect your company from harm.

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

2. Integrity – Compromises to the Trustworthiness of Your Data

We don't hear as much about data manipulation crimes as we do with confidentiality but as hackers become better at gaining entry into systems, the risk of this type of cybercrime is increasing. The motivation of an integrity attack can be to compromise decision making, cause damage to the company reputation, or commit fraud that will result in monetary gain.

Examples include changing the destination for invoice payments or payroll deposits; hijacking communications systems such as email or social media used for unauthorized messages or transactions; or modifying data that will change the outcome of a situation.

Sometimes, entry occurs when an employee uses unsecured methods to access company email and files. Other times malicious code is inadvertently downloaded that opens a door to the intruder.

3. Availability – Denying Access to Your Information

Do a google search for “hospital hacked” and you’ll find a disturbing trend, but the use of ransomware for extortion is not limited to the healthcare field. Sometimes information is the target of an availability attack, and sometimes access to a machine or network is the goal.

Whether it is denial-of-service (DoS), or holding data hostage, the motive can be the payment of ransom or a major disruption of operations that will damage the company’s reputation and ability to do business. The increasing number of devices connected to the internet — from smartphones to manufacturing machinery — has provided more targets for malware and availability assaults. Small businesses might think they are immune from attacks but they are actually easy and plentiful targets.

Common Cybercrime Tactics

Now that you know why cybercriminals may be attacking your system, here are some common ways they will try to obtain your data and ways to notice, prevent, or fix it.

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.

Phishing techniques include embedding a link in an email that redirects employees to a website that asks for sensitive information. That’s one of the more common and well-known tactics. 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 remember?

How to Protect Your Business

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 report to executives how many were opened. This helps you understand how effective your training programs are and refine them to be more interactive and include employee participation. But you should also be using spam filters to recognize and prevent emails from suspicious sources from even reaching the inbox of employees.

To further protect against phishing attacks, ensure passwords are continually reset and that they're complex. You should 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 do have one form of user credential — such as a password — from gaining access to a website.

Malware

Malware is an abbreviation of "malicious software." The software is specifically designed to gain access to or damage a computer. The term refers to a broad swatch of cybercrime tactics including spyware, viruses, worms, Trojan horses, adware, and botnets, all of which can infiltrate a computer and send information stored in the company back to cybercriminals.

How to Protect Your Business

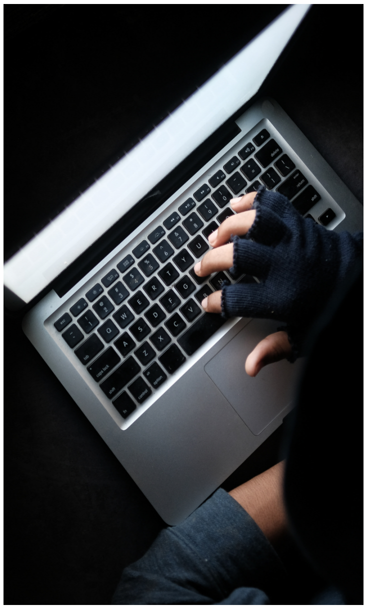
First things first, determine if your machines are already being compromised. After that, stay on the lookout for future attacks and take measures to protect against them.

You'll need to be aware of how the 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. The malware out there today knows to do its work on a computer when the computer is idle, for fear of calling attention to itself. So, when all is quiet, there could be an issue.

One 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 because a huge percentage of malware comes from them. Frequent communication with sites in those countries is a strong sign your IT equipment may be compromised.

Take action to prevent 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.



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 alert users their data has been compromised. What's the logic? As the name implies, ransomware creators profit by holding your data for ransom. 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 Protect Your Business

The first step to protect yourself is to establish best practices that you expect all users to follow. Be sure they're 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.

Identity theft

Identity theft is a fairly well-known cybercrime tactic, though employees are still vulnerable — thus, making 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

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. Since these can take place via social media — scammers pose as people's friends or make up profiles, gain trust, and ask for pertinent business or personal information — you may 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

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 a Business Concern

Assess your risk for cybercrime by first considering the information that you use and store in your business. Then, consider the damage that would result 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 are falling behind in this area is that they lack expertise.

Managed IT Service Providers partner with companies to bring cybersecurity expertise and technology tools to help thwart the growing threat of cybercrime. The best IT support companies include security as a customized IT strategy that is aligned with business goals.

- 82% of SMBs feel they're not targets for attacks as they don't have anything worth stealing.
- But 55% of SMBs admit they've had a cyber attack in the past 12 months.
- 60% of SMB go out of business within 6 months of a cyber attack.

Cyber Insurance to financially recover from an attack and ongoing security awareness training/ phishing tests for all your staff are not enough. Cybersecurity is another business risk leaders need to manage. The good news is you are already adept at tolerating and mitigating such problems as shrinkage, downtime, turnover and waste. These are treated not as threats to the business, but as costs to be managed and avoided.

Don't become a stat line. Protect your bottom-line and your data.

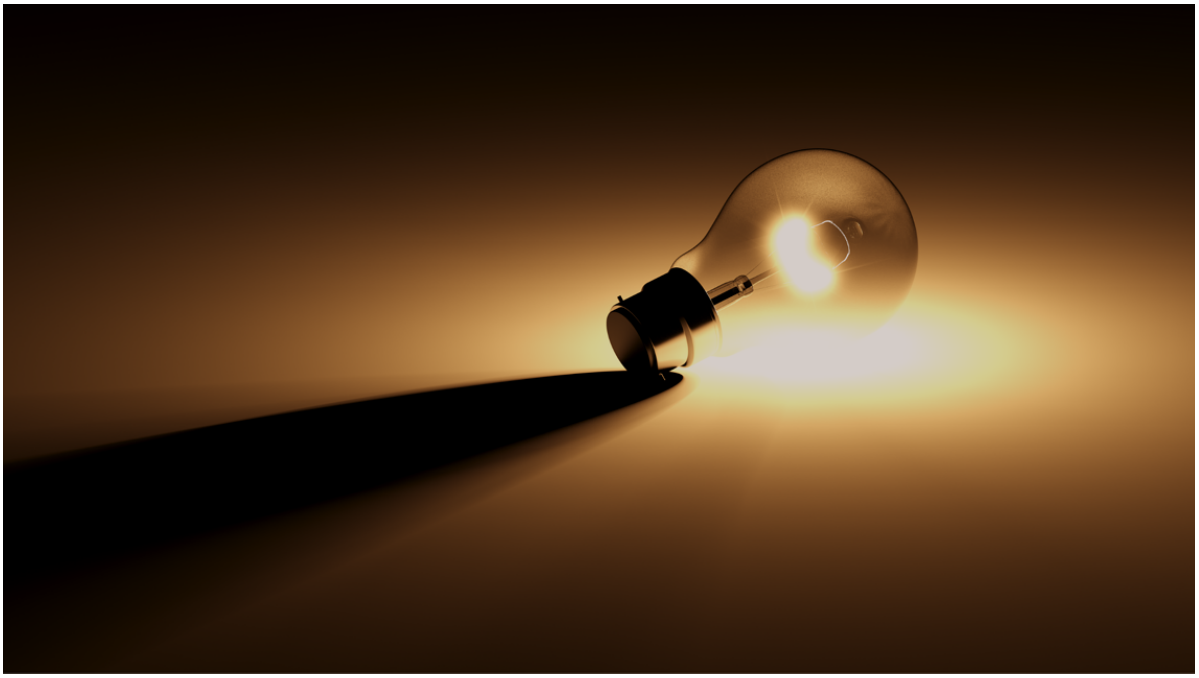
Watch webinar: The Business Leader's Role in Cybersecurity for the Modern Workplace

- CHAPTER 2 -

Security Awareness for Your Business

Security Awareness for Your Business

Cybercrime is projected to be a $6 trillion dollar industry this year, 2021 according to idagent.com.



With widespread news of security concerns, reassurance that your company's solutions are secure is crucial. Awareness of these security issues is one way to protect your business and keep it from happening to you. In early July, there was a cyber attack involving Kaseya which is a software tool used to manage servers and computers.

The same group that hacked the JBS meat processing plants in early June exploited a vulnerability in Kaseya's software in an attempt to hold computers and server's ransom. This is the second incident of this kind of software being taken advantage of with the SolarWinds event in December 2020 being the first.

Attacks on RMMs

Remote Monitoring and Management (RMM) tools like Kaseya and SolarWinds are one of the most secure ways to manage patches and devices, but they are becoming a target for bad actors wishing to exploit others for financial gain.

At Thriveon, we do not use Kaseya or SolarWinds, so there has been no risk to our clients from these events.

That said, we are mindful that we are not completely immune to these types of illegal attempts which is why ardent planning and monitoring is a core function of our business to serve our client base. We work to get ahead of any issues in case there comes a day a software tool that we use might become a target.

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

Preventing Security Attacks

Next-Level Protection

To help avoid becoming a victim of these attacks, it's vital to put multiple layers of security in place and invest in next-level protection with things like multi-factor authentication. Pushing a code to a second device helps to authenticate and protect your account information. Securing your devices and accounts at the jump helps to provide an early adoption of next-level protection. At Thriveon, we internally follow the security measures we recommend to our clients to ensure your security.

Identify and Quarantine

As mentioned, a core business function of ours is to proactively monitor and identify potential risks and mitigate them before they become an issue. We invest in the highest level of protection to proactively pinpoint malicious behaviors and quarantine software and files at the onset of any suspicious activity. We're constantly working day in and day out to take all risks off the table. During this compromise of Kaseya, our protection systems immediately identified and blocked this attack, prior to it being publicly released that it was occurring.

Security Best Practices

We know that the security landscape will continue to evolve, and we are dedicated to staying up to date on the latest in cybersecurity. Following security best practices is a pertinent element to any Managed IT Service provider, so make sure your provider is clearly aligned with following them.

Is your business at risk of an attack?

Ask your IT Group the following two questions:

1. What are you doing to protect our business?
2. What cybersecurity frameworks are you practicing and being audited on?

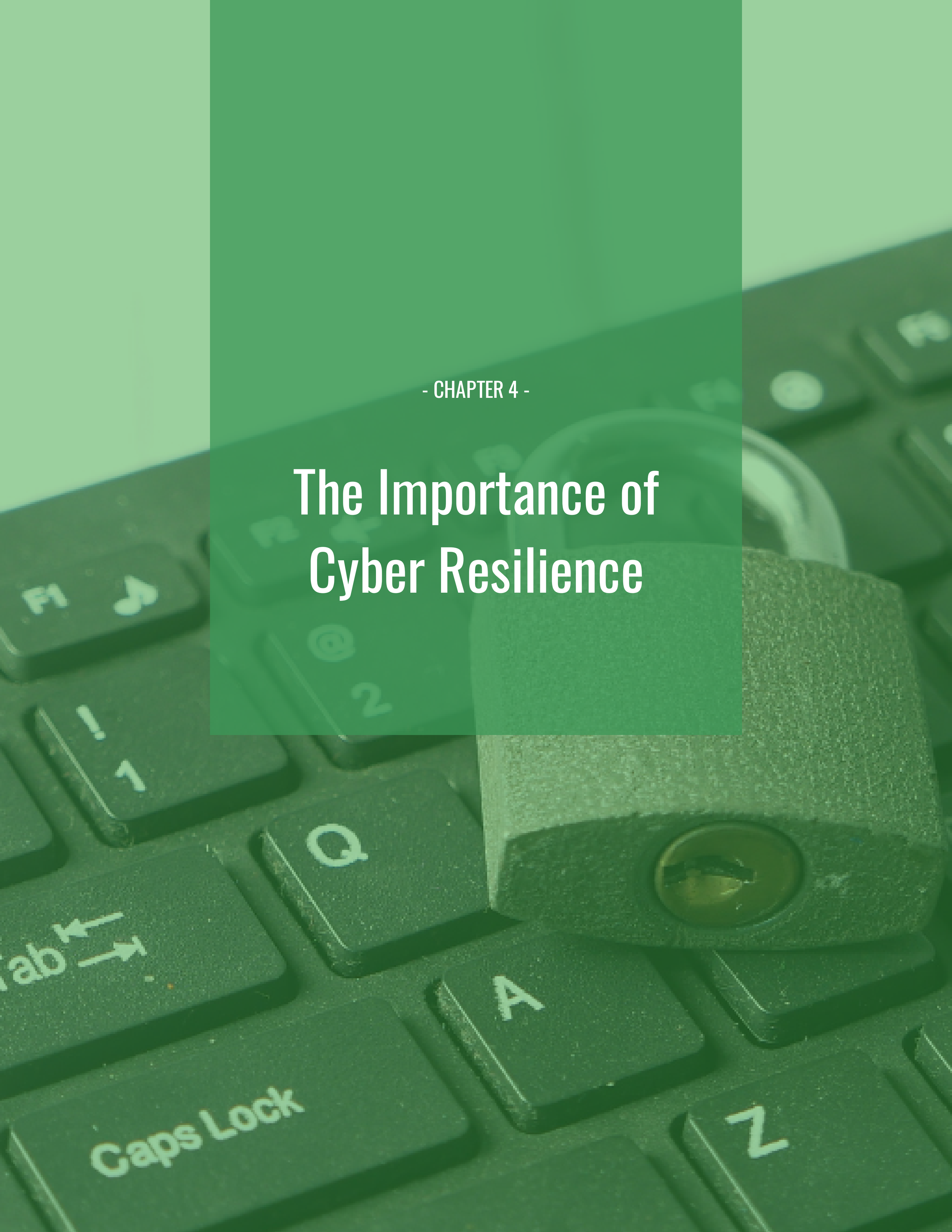
A solid IT firm is implementing new security initiatives every quarter so you can take comfort in knowing that their cybersecurity house is in order. We, at Thriveon, consistently audit and communicate best practices quarterly to our clients, so you'll always be on top of the changes and updates needed to your technology solutions.

Security Trustmark

In 2016, Thriveon secured the Security Trustmark through CompTIA which follows the Federal cybersecurity framework for meeting regulations for the Department of Defense, Financial and Healthcare. We also have regular 3rd party auditing performed to keep our systems in check. Read about the Thriveon difference through our Thrive On IT pathway.

Protect your bottom line and your data.

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



- CHAPTER 4 -

The Importance of Cyber Resilience

The Importance of Cyber Resilience

According to the National Cyber Security Alliance study, 60% of businesses that are hacked go out of business within six months.

The vast majority of damage done in cyber attacks is due to the inability of the company to respond because they have not developed a cyber prevention and response strategy. Think about it. We practice fire drills and earthquake duck and cover drills. Shouldn't we do the same to prepare for risk with similar catastrophic consequences? If your e-commerce system, website, email, customer or operational data was suddenly inaccessible because of an attack, would you be able to get back up and running within minutes, hours, days, or at all? That depends on your business's level of cyber resilience.

Watch webinar to learn how you can better protect your business from falling victim to a cyber attack

What is Cyber Resilience?

The most common definition of cyber resilience is the ability of an enterprise to limit the impact of security incidents. It's a broad approach that encompasses cybersecurity and business continuity management, which aims to defend against cyber attacks and ensure that the business is able to survive. Unfortunately, most businesses fail to develop a plan because they have been lead to believe that having antivirus, firewall, patching, awareness training and backups are enough. I would equate that to having doors that are capable of locking but never get locked.

Cyber resilience includes two primary components. Step 1 includes prevention measures, Thriveon clients enjoy more than 320 of such measures. Step 2 is to develop a plan to take appropriate action if and when an attack occurs. Unfortunately, most businesses fail at both critical steps.

Step 1: Assess the Risks

Before you implement an incident response plan, you'll first need to assess the risks to which your company is exposed. Risks may include*:

- **Strategic** - the failure to implement business decisions that align with the organization's strategic goals;
- **Reputational** - negative public opinion;
- **Operational** - loss resulting from failed internal processes, people, systems, ;
- **Transactional** - problems with service or product delivery; and
- **Compliance** - violations of laws, rules, or

To conduct a risk assessment, you'll need to:

Characterize Your Business

Some questions to ask are: What kind of data do you use? Who uses it? What is the data flow? Where does the information go?

Identify Threats

Common threat types include unauthorized access, misuse of information, data leakage or unintentional exposure of information, loss of data, or disruption or service or productivity.

Determine Inherent Risk and Impact

What would be the impact on your organization if the threat was exercised? Would the impact be high, medium, or low? Regular risk assessments are a fundamental part of your business and they should be reviewed regularly.

Analyze the Control Environment

You typically need to look at several categories of information to adequately assess your business's vulnerabilities. Are your controls satisfactory or do they need improvement? A few examples of controls you might want to look at include:

- Organizational Risk Management Controls
- User Provisioning Controls
- Administration Controls
- User Authentication Controls
- Infrastructure Data Protection Controls
- Data Center Physical & Environmental Security Controls
- Continuity of Operations Controls

Determine Your Organizational Risk

To do this, you'll need to consider how high the threats are and how vulnerable the controls are. From there, you can decide if the risk is severe, elevated, or low. Regular risk assessments are a fundamental part of your business and they should be reviewed regularly. Once you've completed your first risk assessment, you can implement an incident response plan.

Step 2: Develop the Incident Response Plan

Once your team isolates a security incident, the aim is to mitigate the damage. An incident response plan will identify the actions that should be taken when a data incident occurs. The aim of it is to identify the attack, contain the damage, and eradicate the root cause. When your organization responds to an incident quickly, it can reduce losses, restore processes and services, and mitigate exploited vulnerabilities.

The SANS Institutes's Incident Handlers Handbook defines a six-step incident response plan:

Preparation

This step involves creating an incident response team and outlining their roles and responsibilities. You'll also need to develop policies to implement in the event of a cyber attack, as well as a communication plan.

Identification

Decide what criteria calls the team into action, such as a phishing attack. Start to assess the incident and gather evidence.

Containment

Once your team isolates a security incident, the aim is to mitigate the damage. This includes an instant response, such as taking down production servers, a system backup, and long term containment, such as installing security patches on affected systems. Following these steps can prepare your organization for a security incident and ensure that you're taking the appropriate measures.

Eradication

Contain the threat and restore systems to their initial state. This step also includes seeing if the attacker reacted to your actions and anticipating a different type of attack.

Recovery

Ensure that affected systems are not in danger and can be restored to working condition. Monitor the network system to ensure that another incident doesn't occur.

Lessons Learned

Review the steps you took and see if there are areas for improvement. This report can be used as a benchmark for comparison or as training information for new incident response team members.
Following these steps can prepare your organization for a security incident and ensure that you're taking appropriate measures.

Benefits

Cyber resilience can reduce the economic impact on your business after a cyber attack and instill confidence in your customers who know that you are able to protect their data. Consequently, a significant amount of underwriting now takes into account business resiliency.

Adhering to Cybersecurity best practices can prove your organization's resiliency and thus lower insurance costs. With premiums ranging from $10,000 for small organizations to over $100,000 for million-dollar businesses, these cost savings can be valuable.

Ideally, you should implement prevention and an incident response plan before you purchase cyber insurance to better understand what your needs are and how you can enjoy lower rates.

By documenting prevention, detection, and mitigation best practices, you can negotiate better insurance terms and conditions, which may include:

- Reduced premiums
- Broader coverage
- Higher amounts of coverage

In the case of cybersecurity, the offense wins and the defense loses. Getting and staying cyber-secure takes proactive audit and alignment to best practices and real strategic IT guidance and direction. At Thriveon we provide a truly proactive IT service that brings our clients into alignment to best practices and strategically guides their entire technology spend which eliminates issues before they start and allows their business to do more with less.

- CHAPTER 5 -

Is your company's online data secure?

Is Your Company's Online Data Secure?

It's no secret that cybercriminals (also known as "bad actors") are constantly attempting to gather sensitive business data. And while there are a wide variety of cybersecurity systems that aim to keep malicious programs away from your network and employees (like firewalls, spam filters, anti-virus programs and intrusion detection systems), hackers are always developing new and more effective tactics to bypass these defenses and wreak havoc on your company's IT framework. In fact, even if you design and implement flawless technical defenses for your business network, bad actors can still reach your online data by tricking employees into letting them into your system, putting the stability and success of your business at great risk. That's why more and more companies of all sizes and industries are turning toward high-quality managed IT service providers to keep their private information as safe and secure as possible.

Here at Thriveon, we offer peerless IT security consulting and management services, protecting the online data of our clients while helping them attain better business results by leveraging Information and Technology to do more. That's why small to mid-sized businesses across Minnesota utilize our managed IT services to improve their Information Technology systems in order to grow and achieve business success. We also offer our partners the best cybersecurity services in the business, pairing outstanding technical defenses and training with IT leadership to keep them several steps ahead of bad actors. Today, we'll be helping you to determine whether your current IT system needs an upgrade. But before we jump in, let's take a moment to emphasise the tremendous impact an online data breach can have on a growing business.

The Impact of Online Data Breaches

A company's online data can include essential and highly valuable information, such as product designs, customer records, company strategies and private employee information. Bad actors understand that fact all too well, which is why they develop malicious software to make a quick profit off of exploiting this data.

As you might expect, the impact of losing this key information can be absolutely crippling. According to the US National Cybersecurity Alliance, 60% of small companies go out of business within six months of a serious data breach. Why? Because many organizations simply can't recover from the loss of money, productivity and reputation that data breaches cause.

After all, clients and customers alike are highly unlikely to trust you with their private information when they know that your business is incapable of protecting it. Consequently, if you want to ensure that your business continues to thrive, it's essential to develop the strongest cybersecurity system possible.

Assessing Your Company's Security Measures

One of the best ways to determine whether your company's online data is secure is to perform a computer security audit. This is essentially a full assessment of your organization's security system.

Through interviews, security vulnerability scans and monitoring software, a security audit can be used to examine how effectively your employees, computers and servers are protecting your sensitive online data. This process can be time-consuming, but it's a great way to make sure your business's bank information, designs, trade secrets and employee information are being kept safe. Once you've received the results of this audit, you can decide whether your company needs to invest in stronger security measures.

Bear in mind that working with a managed IT service provider like us is another fantastic way to assess the safety of your business's online data. After scheduling a meeting with Thriveon, we can show you how your current IT systems and results compare to some of our current clients, helping you to decide whether your current Information Technology framework needs to be bolstered in order to avoid cybersecurity threats. From there, we'll discuss how our proven processes can be used to create better IT results and optimize security initiatives for your business.

Thriveon's Industry-Leading Security Services

There are four key aspects to Thriveon's top-quality cybersecurity services:

1. **Technical Security Measures**

All businesses require sufficient technical security measures (like firewalls, spam filters and anti-virus software) to keep bad actors away from sensitive online data.

At Thriveon, our IT team is constantly researching and implementing the most effective security systems and processes for businesses. A partnership with us will grant your company access to the best technical security programs in the business, keeping your online information safe and secure by locking it away from outside parties and tracking how it's stored and used by internal staff.

2. **Backups and Recovery**

Experts in the IT field agree that businesses should always develop a backup plan in the event of a data breach. At Thriveon, we've designed innovative backup and recovery systems that record and safeguard all essential business data and programs, allowing them to be restored regardless of what happens to the original assets. This feature will allow your company to get back on its feet and resume operations very quickly, even if a bad actor manages to slip through your IT defenses and steal or delete essential data.

3. **Employee Cybersecurity Training:**

Ensuring that your employees can recognize and avoid malicious files and attempts to steal private information is just as important as having solid technical security measures. Thriveon can provide every member of your team access to quality cybersecurity awareness training, detailed educational sessions that teach employees how to identify and react to deceptive tactics from bad actors, including malicious email attachments and phone calls. We also utilize robust spam filters to sort through and remove a vast majority of malicious content before it reaches your staff, further mitigating the chances of security breaches. Is Your Company's Online Data Secure?

4. **IT Security Leadership and Guidance:**

The best way to leverage an organization's IT strategy and processes is through IT leadership. Thriveon can provide your business with a VCIO (Virtual Chief Information Officer). This highly experienced IT professional will work extensively with your management team to develop and implement smart, feasible IT strategies to meet your company's business goals while ensuring that it benefits from the most effective security measures possible

- CHAPTER 6 -

Optimizing your business' cybersecurity

Optimizing Your Business' Cybersecurity

Considering the devastating effects that cybercrime can have on companies of all sizes and specialties, many businesses executives are looking for different cost-effective strategies they can leverage to protect sensitive information and ensure that cybercriminals are incapable of compromising and shutting down their IT network. However, the world of Information Technology is constantly shifting and evolving as new technologies and best practices come to the fore, making it difficult for many companies to assess which security investments will provide optimal protection, especially those without access to professional counsel from an IT managed services provider.

At Thriveon, we're committed to unleashing your business success through top-quality IT support and counsel. That's why small and medium-sized companies across Minnesota trust in us to keep their IT systems fully protected and operating at peak efficiency. We also understand how challenging it can be to determine the best IT security investments for your business when you're so busy managing daily IT operations and putting out fires. Today, we'll be taking a few minutes to discuss three simple steps your company can take to improve its cybersecurity systems, decreasing the likelihood and impact of system breaches in the process.

Step 1: Update and Refine Your Technical Security Measures

Technical security measures encompass a variety of core resources that protect your business from unwanted and malicious messages and files, including anti-virus programs, firewalls, spam filters and intrusion detection systems. Regrettably, cybercriminals are constantly developing new viruses and malware to worm their way into your company's system to steal information or compromise your business processes. Technical security measures can help manage these threats by tracking the storage and use of your company's sensitive data and creating powerful barriers that prevent cybercriminals from accessing your network through hacking or operating company devices connected to the internet.

Filters, firewalls and security programs are continuously being improved in response to the waves of malware and viruses that cybercriminals create, which is why it's imperative to keep all of your current technical security measures updated. However, it's important to note that the current security systems your company employs might not provide a sufficient level of protection for your business processes and assets.

Committing some of your internal resources toward researching the latest and most effective technical security measures is a great way to pin down which ones your company should consider investing in. Partnering with an IT managed services provider like us is another great option if your internal team is too pressed for time or needs additional guidance.

Step 2: Utilize Employee Cybersecurity Training

Of course, technical security measures alone aren't enough to shut down cybercrime. Even if you invest in state-of-the-art technical defenses, cybercriminals can still gain access to your network through your employees. In many cases, cybercriminals will disguise their malicious software as seemingly innocuous email attachments that they send out to multiple staff members. If your employees attempt to open or download one of these files, they gain complete access to your entire network, resulting in corrupted data, stolen assets and significant business downtime. That's why many businesses provide employee cybersecurity training for their staff to ensure every member of their team is made aware of these veiled threats and prepped on how to effectively deal with them.

Over our years of assisting clients with employee cybersecurity training, we've found that making this initiative a part of your company's onboarding process for new employees works best. However, it's also essential to perform regular, focusing training sessions with all of your staff to ensure they stay updated on the latest cybersecurity threats and cybercriminal tactics, including your IT and management IT employees (cybercriminals will specifically target these individuals due to the wealth of business information they have access to). Establishing and communicating a concrete procedure in the event of a security breach is also critical.

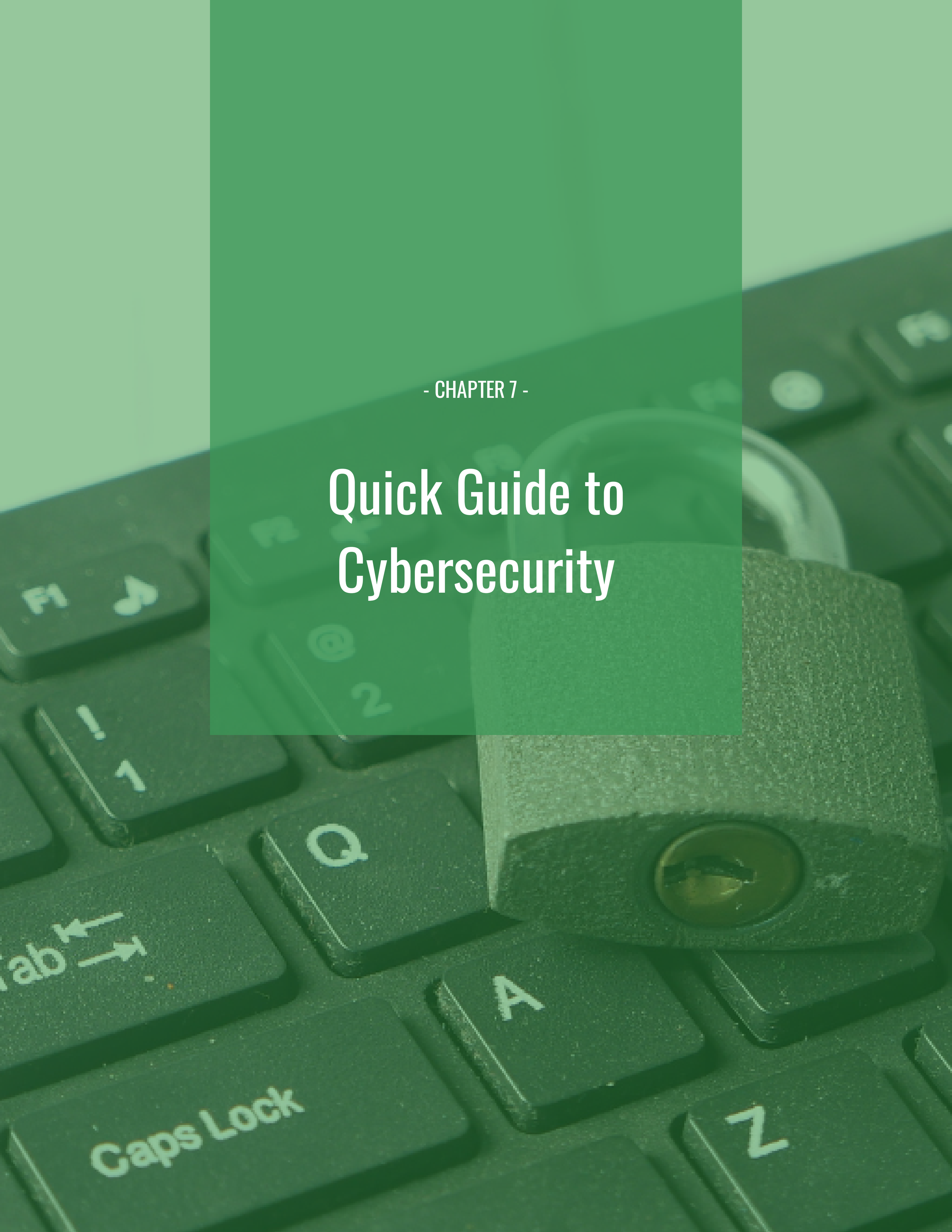
Step 3: Create Backups and Recovery Systems

Unfortunately, no matter how comprehensive your security measures are, it's essentially impossible to create an impenetrable defense for your business's IT network. There are simply too many unknown threats being developed to assume that your company will be 100% safe from all of them. However, thanks to IT backups and recovery systems, you can guarantee that all of your company's essential data, programs and other technology assets can be reclaimed in the event of a security breach. These final lines of defense will ensure that your business can recover and resume its operations even if everything on your current network is corrupted or lost.

Your business can use a host of different data storage mediums to recover its essential assets, including solid-state storage, remote backup services, magnetic tape and hard disks. Each brings a number of potential advantages to the table, so be sure to check in with your internal IT team for guidance if needed. Partnering with an IT managed services provider is another great way to pin down which specific backups and recovery systems will work best with your company's current IT framework.

Is Your Company's IT Network Safe Now?

Almost every managed IT provider you meet with will discuss the basic security measures we've listed above and offer to implement them into your current IT system, claiming that these tools are the best defenses your business can bring to bear against cybercrime. And that's exactly why these providers aren't equipped to protect your company. After all, it takes more than a series of reactive systems to keep your business safe from cybercrime. Here at Thriveon, we combine IT strategy with a proactive, process-driven approach to identify and manage cybersecurity threats before they get the chance to affect your system and slow down your employees. In fact, our Proven Process is so effective that we've prevented 100% of ransomware and network breach attempts for our clients this year.



- CHAPTER 7 -

Quick Guide to Cybersecurity

Quick Guide to Cybersecurity

Cybercriminals are always looking for opportunities to take advantage of outdated business IT systems. This allows them to spread malicious software in order to steal sensitive financial or customer data. Bad actors (an industry term for cybercriminals) can also utilize denial of service attacks to overload business computers and prevent them from functioning properly, inhibiting productivity and profitability. Moreover, according to the US National Cybersecurity Alliance, these attacks are so devastating that 60% of small companies go under within six months of a serious data breach, which is why it's imperative to invest in top-quality cybersecurity measures to keep your organization a step ahead of bad actors and their ever-changing tactics.

At Thriveon, we take pride in offering small to medium-sized businesses across Minnesota with all of the resources and support they need to grow and thrive. Our team provides industry-leading managed IT services and Information Technology security solutions that leverage our expertise to help clients mitigate the risk of cybercrime and achieve their business objectives. We also understand that it's almost impossible to ensure optimal security without help from IT experts, especially when you're busy juggling technology management with running your business. Today, we'll be teaching you more about cybersecurity and what your company can do to bolster its defenses against cybercrime.

Is Your Business Prepared for a Cyberattack?

Many business leaders make the mistake of assuming that their current IT team already has the knowledge and time required to identify and manage potential threats. Regrettably, most small internal IT teams need to commit almost all of their efforts on putting out fires and keeping daily operations running smoothly, making it very difficult for them to research and implement the latest and greatest cybersecurity systems and practices. B

ad actors often take advantage of this fact by targeting smaller businesses, knowing full well that their IT teams don't have the resources to assemble a sufficient defense. To exacerbate matters further, the crippling effects of a successful cyberattack (including business downtime, lost productivity, loss of company assets and the costs required to clean up the breach) put even more strain on an internal IT team's time and budget, inhibiting recovery and leaving the door wide open for the next threat.

It’s also important to note that each and every member of your business plays an important role in preventing successful cyberattacks. In fact, we’ve found that training employees on how to recognize and respond to potential cybersecurity threats is just as important as developing a solid technical defense. Many cybercriminals targeting businesses use tactics that hinge on tricking employees into opening the door to your company’s network for them.

In many cases, hackers will use phishing emails and fraudulent telephone calls to manipulate employees into revealing their username and password, effectively getting them past your network firewall. From there, bad actors have access to any and all company assets, including product designs, customer records, company strategies and sensitive employee information, allowing them to steal, alter or delete any data they wish. Put simply, if your current internal IT team isn’t providing detailed security training and guidelines for your employees, then your business is at risk, regardless of how advanced or powerful its technical defenses are.

Strengthening Your Organization’s IT Security

There are four main aspects to developing a strong, secure cybersecurity system for your business. Here’s a brief rundown on each to give you a better understanding of what they entail:

1. **Technical Security Measures**

This facet of cybersecurity involves key technical layers, such as firewalls, anti-virus programs, spam filters and intrusion detection systems. These applications are almost always large investments, which is why it’s critical to determine which ones will work best for your organization before purchasing them. If your internal IT team is too inexperienced or pressed for time to manage these decisions, then you should strongly consider partnering with a managed IT service provider like us. Thriveon’s team of IT professionals is always researching the most efficacious security software and practices, allowing us to support your internal staff with high-quality guidance and counsel.

2. **Backups and Recovery**

No matter how strong your organization's current cybersecurity setup is, it’s impossible to provide 100% protection from every single threat. Hackers are perpetually developing new programs and tactics to attack businesses, which is why it’s imperative to develop an emergency plan in the event of a security breach.

For example, Thriveon utilizes unrivaled recovery and backup procedures to guarantee that our clients' critical data isn't deleted. A partnership with us will allow your company to resume business operations quickly and effectively even if a hacker slips past its concrete security measures.

3. **Employee Cybersecurity Training**

Once again, training your employees on how to identify and avoid potential online threats plays a pivotal part in decreasing your organization's risk of a successful breach. Luckily, cybersecurity awareness training doesn't have to be time-consuming or expensive, especially when you work with Thriveon. Our robust employee education and training practices aim to develop consistent, predictable behaviors that keep your team safe from bad actor tactics.

IT Security Leadership and Guidance:

VCIOs (Virtual Chief Information Officers) are dedicated Information Technology professionals who work with businesses to develop smart, feasible IT strategies and initiatives to maximize the effectiveness of cybersecurity efforts, making them a huge boon for executives without the time or experience needed to manage and guide the organization's IT systems. VCIOs can collaborate with your company's management team to identify key security weaknesses and pin down opportunities to improve them without throwing your IT budget out of control. Thriveon provides a highly qualified VCIO for each client.

Interested in Learning More About Cybersecurity?

If you want to learn more about cybersecurity and what you can do to optimize your business's current protection system, then be sure to check out our Knowledge Center. It includes helpful resources on a variety of IT topics, including a free e-book on how to optimize your organization's cybersecurity infrastructure by establishing practical employee guidelines.

- CHAPTER 7 -

Helpful Security Hints

Helpful Security Hints

Do:

- Have Cyber Insurance: This will help you to financially recover from an attack
- Provide ongoing security and phishing training
- Make updates to anti-malware, computer operating system and firewalls
- Be overly cautious with odd emails and links and attachments in emails: Check the spelling of email addresses and links by hovering your mouse over it
- Implement Click Protection so if you or your team happens to click on a bad link, it is less likely to hijack your system
- Have unique complex passwords for every login. Easily track this by using a Password Manager
- Call to verify ACH payment requests the first time or if there is a change

Do Not:

- Do not click on any suspicious attachments in emails
- Do not click on web page advertisements: These can download malware
- Do not add your contact information, potential password recovery answers or bank account details to your social media or other public sites
- Do not save or store passwords on your web browser or computer
- Do not keep a company list of passwords
- Do not use public Wi-Fi
- Do not use public computers

Security Trustmark

In 2016, Thriveon secured the Security Trustmark through CompTIA which follows the Federal cybersecurity framework for meeting regulations for the Department of Defense, Financial and Healthcare. We also have regular 3rd party auditing performed to keep our systems in check. Read about the Thriveon difference through our Thrive On IT pathway.

Protect your bottom line and your data.

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

THRIVEON
INFORMATION & TECHNOLOGY

Schedule a Consultation

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

Schedule a Consultation