THE SMALL BUSINESS GUIDE TO CYBERSECURITY 2023

How to secure your small business so you can proactively protect from cyber threats

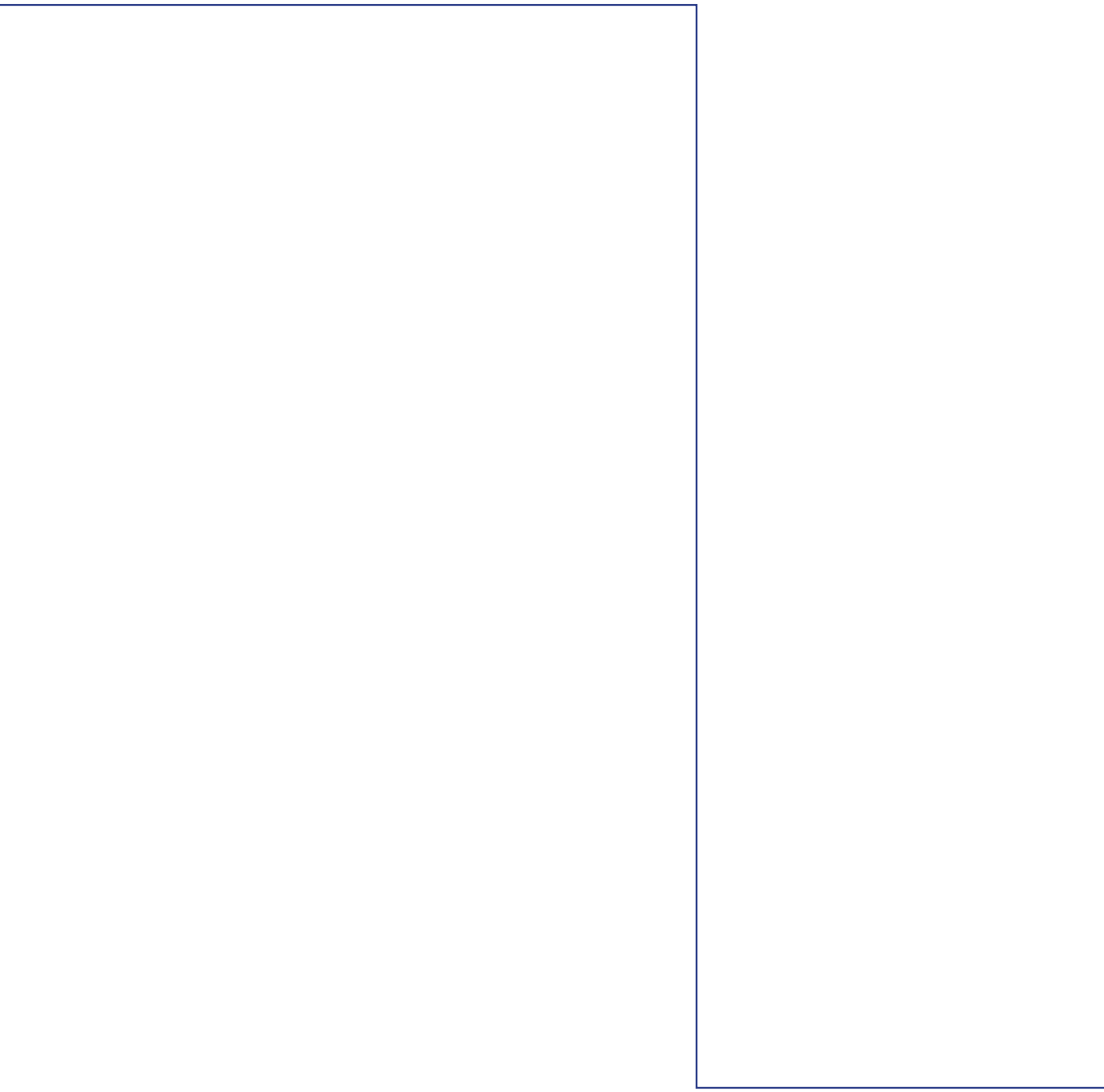
LIGHTHOUSE
TECHNOLOGY SERVICES

ABOUT LIGHTHOUSE

Lighthouse Technology Services connects companies in need of technology talent with the right technologists for their businesses, and we've been at it since 2004.

Headquartered in beautiful Buffalo, NY, on the shores of the Great Lakes, and in the midst of Niagara Falls, we serve as a guide to companies looking for technology help, and as a beacon to talented professionals looking for a partner on their technology work journey.

TABLE OF CONTENTS



INTRODUCTION

Cybersecurity is one of the top concerns for businesses across the United States looking to 2023 and beyond. The complexity of business networks and the number of devices connected to those networks create more potential vulnerabilities every year, and hackers and cyber attackers are constantly finding new ways to gain access to these systems.

For small business owners especially, the impact of a data loss or network breach can be catastrophic.

But what aspect of cybersecurity and protecting systems and data that isn't discussed as much?

The human impact. Your customers who can feel deeper trust in your business, knowing their data is protected. Your team members who can work confidently, with tools and policies in place to keep their work protected.

The range of cyber threats is growing, and we want leaders like you to feel confident that you have the tools necessary to succeed in this environment.

Knowledge is power, and we hope this Guide to Cybersecurity leads you to a proactive mindset when it comes to protecting your business.

Each chapter of this guide helps you dive deeper into specific aspects of cybersecurity to protect your business, including cyber insurance, vulnerability scans, multi-factor authentication, antivirus, and much more. We'll start with an introduction that covers your bases, a series of 11 questions to help you get the right context on where your business stands today.

1. Do you have an accurate inventory of your IT environment?

If you don't know you have it, then you can't protect it. And complete awareness of your technology inventory is the first step in cybersecurity readiness.

All hardware, such as company desktops, laptops, mobile devices, and routers needs to be inventoried. This includes employee devices used for business purposes if Bring-Your-Own-Device (BYOD) is a part of company policy.

And you'll want to include a current list of all software and applications you use - get the entire technology environment mapped and documented.

Remember, your technology environment will evolve over time, so plan on updating your inventory asset map on a regular basis.

2. Have you performed an IT risk assessment?

Once you have your complete IT inventory mapped for your company, the next step to Cybersecurity Readiness is to perform an IT Risk Assessment.

An IT risk assessment identifies the Cybersecurity Risks that your company faces given the current state of the company's IT Inventory, IT setup, and industry.

Such an assessment goes beyond the company's hardware and software. It also addresses the company's data assets, and industry-specific or work-type-specific compliance standards and regulations, like HIPAA, PCI, and SOC2.

For one example, manufacturing companies can be at risk because of their role played in the supply chain, which is one reason many enterprise retailers and large end-point customers require risk assessments of their manufacturing suppliers.

3. How have you secured your network?

Once you understand your biggest cybersecurity threats, it's time to secure your network.

Active firewalls, antivirus, and malware protection tools all play a vital role, but they are just the beginning of complete protection for your business.

The setup and management of your company's Wi-Fi will play a critical role in security. Tactics like rotating passwords for your Wi-Fi, using separate guest and business networks, and limiting how long someone can be online using the guest network, are just a few of the steps that could be implemented to keep the company's network safe.

Remember, we're also living in a remote-work world now. The networks your team connects to outside of your physical office space can open the door to additional cyber threats.

4. How do you limit user access?

Most employees do not need master access to the company's software tools and applications to do their job. But many companies grant such access to users by default. And this is a simple but important cybersecurity hole to close.

Manage your users' access privileges. Most technology tools have user access settings that can be customized or restricted for security and safety.

To return to our manufacturing example, a company's ERP solution is a great example of this. Give team members the ability to access only the portions of the application they need to complete their work tasks. This follows the Principle of Least Privilege for restricting access rights. And limiting user access can minimize the damage caused by a breach.

5. What tools and policies are in place to protect your data?

You can better protect customer, employee, and proprietary data by implementing helpful cybersecurity tools and policies in areas like password protocols.

Your business might encourage users to use password generators to ensure password complexity, or enable the use of an encrypted password manager to securely store hard-to-remember passwords or vary passwords for each employee's online account.

Administratviely, you can require password changes on a scheduled timeline or when data breaches occur. And tools like multi-factor authentication add a layer of protection to your user access.

6. Do you have a policy for updating hardware and software?

Maintaining, updating, and patching current web browsers, software, and operating systems strengthens your security profile.

Secure businesses update their technology to block attacks when threats or vulnerabilities are detected. And if you ignore an update notification, you could be leaving your business at risk.

In the same vein, relying on old technology is a very risky move. Bad actors target legacy infrastructure in the cyber world, because security support is no longer updated or provided to hardware or software after a certain amount of time.

7. Is your data backed up effectively?

Having a backup plan will help prevent your business data from being lost in the event of a disaster. Data backup best practices include:

- Implementing a data backup process
- Keeping more than one data backup
- Encrypting data backups
- Limiting access to your data backups
- Monitoring and managing backups
- Testing Your Backups

Automated and regularly scheduled data backups can help you through a hack or other emergency. But don't rely entirely on automated backup solutions because something could go wrong, and you might not know until it's too late and valuable data has been lost.

8. What plans do you have in the case of a cyber disaster?

Data loss and down systems can happen for a number of reasons, but your company's data and systems recovery will go smoother and faster if you proactively document, evaluate, and test a Business Continuity and Disaster Recovery Plan.

Document the steps you will take in the event of a breach occuring or a natural disaster striking, and pre-determine who is responsible for each step in the process.

Decisions on how to return to business as usual will be more clear and free of stress and conflict if you put a process in place first.

There's no need to be unprepared in a business crisis.

9. What education have you provided to your team?

Employees are often the weakest link in a company's cybersecurity chain.

Mistakes happen, as does carelessness, so making ongoing cybersecurity training and awareness a priority is an important step in Cybersecurity Readiness.

There are even tools to safely test your employees' ability to identify phishing scams and ransomware.

10. Are your business partners also secure?

Today, our businesses are digitally interconnected and cybercrime is at an all-time high. Because of this, more and more companies are requiring good cybersecurity hygiene, not just of themselves, but of their suppliers and vendors.
And you should too.

The requiring of Certificates of Insurance (COIs) denoting cyber insurance coverage and the sharing of cybersecurity practice documentation are new common standards for doing business with enterprise companies, and these demands are flowing down to the small to mid-size business space.

In manufacturing, the integrated supply-chain mentality especially, is driving these actions.

11. How do you identify threats and create efficiencies?

Your company's technology environment is living - it's growing, dying, and will change over time. Hardware will come to its end of life, systems will become outdated, and once protective tools will become obsolete in the face of new technology that will take its place. And to be sure, cybercriminals will find new vulnerabilities and new techniques to commit cybercrimes.

Continuous scanning and monitoring for threats is an important component of good cybersecurity hygiene. And staying informed about new threats can help your company be proactive in keeping up defenses.

At the same time, managing your company's technology environment with an eye on efficiency building can go beyond security to assist your company in reducing costs, saving time, improving employee retention and customer satisfaction, and much more.

TAKE CONTROL OF YOUR COMPANY'S CYBERSECURITY CARE

Ready to get started? Hopefully we have given you a foundation from which you can start and structure your company's cybersecurity action plan.

In the following chapters, we'll outline different circumstances and situations that affect how companies like yours can and should tackle cybersecurity, and address topics like supply chain and cyber insurance requirements.

When you're ready to start building your own cybersecurity plan, open up a copy of our Cybersecurity Workbook for 2023.

1

HOW TO AVOID GETTING YOUR CYBER INSURANCE CLAIM DENIED

With digital threats on the rise, more businesses are viewing cybersecurity insurance as a priority or a necessity, not just something that's nice to have. It's especially become more important in a post-COVID business world.

Still, a cyber insurance policy is just a starting point to protect your business. There are certain expectations these insurers look for businesses to meet to avoid claims being denied.

Almost All Cyber Insurance Policies Have Exclusion Clauses

Under certain circumstances, cyber insurance policies will not cover all liability for your business. Some of these common exclusion clauses include:

- Employees acting outside the scope of their work
- Wide-spread digital viruses impacting many businesses
- Regulatory and legal challenges, and related penalties
- Physical damage to company property

Cyber insurers may deny a claim if they find "a failure to maintain" or "failure to follow," both the online version of negligence, certain minimum-security standards and practices as outlined in the insurance policy.

What steps can you take now to meet your company's requirements for cyber insurance?

Show a standard of care in cybersecurity

Insurance companies want proof that your business is taking proper precautions to prevent cyberattacks. And if you haven't taken the necessary steps to protect your company's digital infrastructure, there's no guarantee your insurance claim will be granted.

Here's what to do to prevent the chances of a cyber insurance claim denial:

Step 1: Map out your company's entire technology landscape, so the insurer can understand the scope of your digital presence. It's a good practice to document everything you hope to cover under cyber insurance.

Step 2: Show your insurance carrier the proactive protection tools you have in place. And if you don't already have them, consider implementing endpoint or managed detection and response, also called EDR and MDR. Relying on antivirus software alone is unlikely to satisfy your insurance provider.

Step 3: Show the insurance carrier the steps you've taken to protect your supply chain. In 2013, retailer Target was infiltrated through a security breach from their HVAC vendor. 40 million debit and credit card records belonging to Target's customers were compromised, and the breach was estimated to cost over $200 million. The connections between businesses and their vendors remain a risk, and many companies are requiring their suppliers to show proof that cybersecurity protocols and insurance are in place.

Step 4: Show that you're training your employees to follow cybersecurity protocols. Human behavior is the highest cybersecurity risk, and insurers will want to know what programs you have put in place to reduce that threat. Password policies, device management policies, and education on how to avoid malicious links are some ways to avoid the top causes of cybersecurity breaches.

What technology tools should you expect to have in place?

In addition to those already mentioned, insurers will look for:

- Encryption software
- Multi-factor authentication software
- Device security solutions like virtual private networks (VPN)
- An established data backup process
- Documented policies for how your company will respond to cybersecurity incidents and breaches

And remember, cyber insurance evolves over time. As work culture has shifted to more remote and hybrid work environments, insurers are constantly reviewing their cyber insurance requirements to account for new risks. We're currently seeing a major shift in the cost and requirements of cyber insurance policies. What was once covered under a cyber insurance policy may be declined a year later.

The best way to prevent a cyber insurance claim denial is to take action and ensure you have the right tools, trainings, and procedures in place to protect yourself from cybercrime.

2

UNCOVER CONFIGURATION THREATS WITH A VULNERABILITY SCAN

The risk of a cyber breach grows as the number of devices connecting to a business's network surges. Now, more employees bring their own devices to work and a greater number of people are working remotely, both of which pose additional threats to a company's security when employee devices connect to the company's network and data.

Each device brought into the company's network is configured differently. **That configuration** is a key focus when we think about cybersecurity.

Some devices may have configurations in place to restrict the sharing of important data. Others may have configurations open and set to sharing all data. And it's these configurations on company or employee devices that can act as open doors and windows for cyber criminals to climb through.

How does a business maintain control over those configurations?

Yes, it's difficult for companies to manually monitor what devices are connected to their network and the configuration of each connected device. And yes, misconfigurations can be difficult to detect. But a **vulnerability scan** can help detect insecurities in your systems and software.

An automated vulnerability scan proactively identifies network, application, and security vulnerabilities. This process aims to find any points of entry, and it also predicts the effectiveness of any countermeasures you may have in place.

The scan detects and classifies flaws in individual devices, communications equipment, and overarching networks, and then compares details about those vulnerabilities with a database of known exploits. Many vulnerability scan programs cover issues like bugs in code, packet construction anomalies, default configurations, and other known flaws in your system.

An IT managed service provider will have the tools to perform these scans for you and can take several scanning approaches.

First, to scan your external exposure, they'll look at all applications, ports, websites, services, networks, and systems facing the internet. Second, they'll run an internal scan, identifying system and application security holes that cybercriminals might exploit once they get in. Environmental scanning considers any connected desktop and mobile devices, websites, and cloud-based programs.

It's critical you secure your company's network, devices, and data. Identify system security holes in misconfigurations with vulnerability scanning before the bad guys find them.

3

THE BASICS OF FIREWALL PROTECTION

Let's start here: what is a firewall? It is a security device that protects networks and allows data to pass between computers or network devices according to predetermined rules.

A surprising number of businesses are operating without firewalls, which can lead them into disaster if they don't have one up-to the test protecting their business networks from outside attacks; assumptions may be made about what kind protection will do instead unfortunately resulting in limited scope overall protection for your important assets like customer information!

Filtering is one of the most important functions of a firewall. A strong firewall actively looks for known viruses, phishing emails, and spam, and then blocks them before they can get past. The firewall identifies patterns over time and adjusts its protective capabilities along the way. Business firewalls also monitor data in both directions. When a computer goes

online, all the data coming in and going out from the device is inspected to see whether it's safe or not. If it doesn't pass the test, the firewall can instantly block it and record the details in a log. This is an important function because it gives the firewall the necessary visibility to protect businesses from cyberattacks.

Controlled Performance is the capability to use your firewall to set network traffic priorities. Rules can be set to allow certain applications to be treated as a higher priority than others, certain departments or even users. With these rules, you can tailor your company's network performance to meet your unique business needs.

Your firewall is the first line of defense against attacks, and it can also be used to improve network performance. In most cases, the out-of-the-box default settings will suffice but, in some cases, you may need to fine-tune your firewall's rules to get the most out of it. If you have a specific need for Controlled Performance, then working with a professional to configure your firewall is recommended. By putting the right rules in place, you can expect an improvement in network speed and reliability.

One of the most important features of a business firewall is oversight. With a business firewall in place, you have complete viewership over your network. This means you can see exactly who is accessing what, and when they are doing it. That level of visibility is essential for preventing security breaches.

Business firewalls allow you to create rules for specific users, devices, and times. For example, you might allow your employees to access Facebook during lunch breaks only, while at the same time keeping it completely unblocked for your marketing team. This level of flexibility is essential for ensuring that your employees are productive, while also keeping your network secure. Finally, business firewalls automatically keep thorough logs of all activity. If a security concern does arise, you will be able to identify it quickly and take appropriate action. In short, business firewalls provide an essential level of oversight for your network.

A strong firewall is essential for allowing your remote workforce to access your business systems and data securely. Since the outbreak of COVID, remote work arrangements have become increasingly popular, often requiring server access at a moment's notice. A firewall can help to authenticate the identity of users before allowing access and create a virtual private network (VPN) that keeps any transferred data safe from interception. By ensuring that only authorized users can access your servers and that data is properly encrypted, you can help to keep your business safe from cyber-attacks.

4

KEEP YOUR DATA SAFE WITH MULTI-FACTOR AUTHENTICATION

Businesses of all sizes can become a target for cybercrime. In fact, 61 percent of small businesses have been hacked in the past year. And while there are many steps you can take to protect your business, one of the most important is using multi-factor authentication. Multi-factor authentication adds an extra layer of security to your account by requiring more than just a username and password to log in. This makes it much harder for criminals to gain access to your data. So if you're not already using multi-factor authentication, now is the time to start.

According to a recent study, the average person has over 90 passwords. With so many passwords to keep track of, it's no wonder that many people use the same password for several different websites. However, this can be a major security risk.

If somebody manages to figure out your password, they will then have access to all of the websites that you've logged into with that password. Thanks to social media, it's easier than ever for someone to find out information about you that can be used to guess your passwords. For example, many people use their pet's name as a password, and this information is often readily available on social media. Security questions can also be easily bypassed if somebody knows enough about you.

Fortunately, there is a way to help protect your passwords and other sensitive information. Multi-factor authentication (MFA) is an additional layer of security that can be used when logging into websites and other online services. With MFA enabled, you will need to provide two forms of identification in order to log in - typically something that you know (such as a password) and something that you have (such as a physical token or your smartphone). This makes it much more difficult for someone to gain unauthorized access to your account. While multi-factor authentication is not foolproof, it is an important step in protecting your online information.

Amazon, Facebook, Gmail, and other websites offer Multi-Factor Authentication to help protect your information. MFA is a must-have for online banking, email, and online shopping. It's also critical for cloud storage accounts (like Dropbox or Sync), password managers, communications apps, and productivity apps. Especially, if you use the same passwords for different websites and apps.

Multi-Factor Authentication adds an extra layer of security by requiring you to enter a code from a text or email before logging in. This ensures that only you can access your account, even if someone knows your password. Amazon, Facebook, Gmail, and other websites make it easy to set up MFA. Once it's enabled, you can rest assured that your account is safe from hackers and thieves.

Even if a hacker manages to capture your login username and password, they will still be required to possess a second device, like a cell phone or additional email, in order to gain access to your accounts. This makes it much more difficult for hackers to breach your account.

Additionally, you will usually be notified on your second device when someone is trying to log into your account, so you can be sure that it is not someone who should have access. Multi-Factor Authentication is an important step to take in order to protect your online accounts.

As businesses continue to rely more and more on digital technologies, the need for strong cybersecurity becomes even more critical. With multi-factor authentication, companies can easily protect their data and keep their networks safe from hackers and other cyber threats. By using this additional layer of security, companies can ensure that they are doing everything they can to keep their data secure.

Take the necessary steps to safeguard your information so that you can help reduce the risk of data breaches and other cyber incidents that can have serious consequences for businesses. If you want to keep your data safe in today's digital world, it is essential to use multi-factor authentication for better cybersecurity.

5

FIVE THINGS YOU NEED TO KNOW ABOUT SUPPLY CHAIN ATTACKS

Supply-chain attacks may not grab the headlines in the same way as ransomware or data breaches, but these sneaky cyberattacks are just as dangerous for your business.

The supply chain covers refining, manufacturing, packaging, and transportation. And supply-chain attacks in the IT sense are cyberattacks that see bad actors target vulnerabilities where businesses connect to one another. A supply-chain attack exploits a weakness at the target company's vendor.

In one well-known example, hackers stole 40 million financial records from the American brick-and-mortar retailer, Target. The hack caused Target's company profits to fall by 46 percent after they announced the news. But the attackers didn't attack Target directly. Instead, they obtained credentials for Target by breaching one of Target's small heating and air conditioning suppliers.

A supply-chain attack can occur in any industry. And today, the problem is getting worse as businesses grow more interconnected. So, here are the top five things you need to know about supply-chain attacks to protect your business.

What is a supply chain attack?

A supply-chain attack is opportunistic, gaining access to one business by finding a vulnerability in another. It occurs when someone gets into a system through access to a supplier or service provider.

Instead of attacking an enterprise directly, cybercriminals attempt to identify and exploit a weakest link. And as businesses become more digitally interconnected, the attack surface grows larger with the addition of suppliers and customers connected to the enterprise.

Many businesses today are providing network access to a software vendor, payment processor, cloud backup solution, or to customers and suppliers via installed applications and connected devices. A compromise at any one of these could give a bad actor access to your business network, and in turn access to one of your customers via your network.

What makes supply-chain attacks so dangerous?

For one, they can happen to any business. From critical infrastructure entities to financial services firms, every business connects to supply-chain partners. The growing complexity of IT compounds attack risks. And while many business owners don't know the details of how their technology integrations work, they assume themselves safe from cyber vulnerabilities.

But they're not safe. And hackers prey on this ignorance.

Plus, these types of attacks are attractive to hackers because they allow them to hit many businesses at once - upping the potential score, since supply-chain vendors often store data for more than one client.

Why are supply-chain attacks growing?

According to a study by Symantec, supply-chain attacks increased by 78 percent in 2019. Why? Because digital interconnectedness and relying on third-party solutions was becoming increasingly common in business. And this was before COVID!

Now, digital transformation has reshaped how we do business with each other, with digital interaction and integration a must. Plus, a digitally integrated supply chain is more efficient, productive, and cost effective.

In addition, by leveraging real-time digital data, quality decisions can be made faster and more reliably. So, more businesses want the integration built into the supply chain.

Cybercriminals know this.

And they know digitally integrated supply chains mean more people have and need access to sensitive data. Plus, small businesses are less likely to have strong cybersecurity protocols and tools in place to defend against their attacks - making them a great side door into a larger payday of data from an enterprise company, as in the case of Target.

Still unconvinced supply-chain attacks are a big deal?

In early 2021, President Biden instituted an Executive Order devoted to researching and identifying solutions for strengthening United States supply chains, including defending against supply-chain cybersecurity attacks.

How Do Supply-Chain Attacks Happen?

There are several ways to breach a supply chain. And the top three methods are:

- Exploiting networking vulnerabilities
- Leveraging unpatched software
- Social engineering

No one is going to let an attacker access their systems intentionally, but small businesses across the supply chain can be slow to update software and antivirus protection. Without the latest protection against formidable threats, your business is at greater risk.

Relying on legacy equipment also makes a business vulnerable. With budgets tight and processes working fine as is, businesses often resist or procrastinate on upgrades. But using a system or device past its end-of-life is bad news because the manufacturer has stopped offering support and security updates on the equipment.

And attacks can come from numerous places. A 2017 breach at Equifax cost the credit reporting company nearly $2 billion. The hackers preyed on an unpatched vulnerability on a consumer complaint portal.

How can you guard against supply chain attacks?

▪ ***Vet your vendors:*** You can't simply trust that your business partners are as determined to secure their network as you are. Ask vendors to share documentation on what security controls they have in place and how they manage risk. This will help you identify if they are taking cybersecurity seriously. Plus, you can assess whether their actions are compatible with your own.

▪ ***Consider compliance:*** Insist that partners have standards of care regarding cybersecurity. Depending on your industry, you may even have regulatory security frameworks to comply with. Make sure all parties in the supply chain are compliant and possess appropriate security posture.

▪ ***Limit access:*** When you do enter a partnership with a third-party, be sure to limit their access. Use the least-privilege approach. This means the vendor has permission to access only pre-determined sites or systems. This helps prevent software from communicating with malicious command and control servers. In addition, set up alerts for third-party credentials that signal when something is out of the ordinary.

▪ ***Know what's connected:*** The inventory of connected devices on your network needs to be known and monitored. Perform an audit to get a full list of all open-source and other types of software, hardware, and systems. With this in hand, replace or remove any outdated systems, services, and protocols.

▪ ***Remove unapproved technology:*** You may tell your employees not to download unauthorized apps onto your IT infrastructure, but they do it anyway. Root out any unapproved IT – also known as shadow IT – as it puts your business at risk.

▪ ***Deploy patches:*** Does your business have patch management and software update processes in place? Don't ignore that notice to install the latest version of a system or application. You could be missing out on plugging a major security hole that the manufacturer has found and fixed.

▪ ***Keep up with vulnerabilities:*** According to IBM, third-party vulnerabilities caused 16 percent of all data breaches in 2020. These attacks are a sneaky way to get the job done. Keep an eye on industry news and cybersecurity notifications from industry and government agencies. Awareness is half the battle.

6

HOW TO SAFEGUARD YOUR BUSINESS FROM EMAIL BREACHES

Email security is a critical component of protecting your business's digital information. Many cite email as one the most important business security threats to address, due to the often-flawed combination of employees, human behavior, and password access.

But is your business doing all it can to prevent email breaches?

- Can you verify that all company and employee passwords are strong?
- Are you prompting your team to regularly change their email passwords?
- Are employees required to create unique passwords each time they update?
- What spam and phishing protection tools have been put in place?
- Have you educated employees on how to identify a malicious email?

No matter what the industry, businesses are always at risk. Scammers send emails and set up spoof domains to get employees to enter access credentials online. These practices have become so common that you've likely experienced this yourself or know someone who has fallen victim to these tactics. And now criminals can buy leaked emails and passwords from a previous data breach.

As an example, cybercriminals can identify which payroll software your business uses. They can visit that payroll website and employ the "forgot the password" option on the credential entry point of the site. Password reset instructions go to your email account, which they've already hacked into. So, they follow the steps, delete the email, and take control of your business's payroll account.
It's that simple.

Criminals will also impersonate you and send invoices to your vendors or customers. They might send an invoice that looks like a genuine one, but with a payable account that's

fraudulent. They'll send emails to your accounting department on your behalf, asking for a payment to be made to a fraudulent account.

And these attacks are working for cybercriminals. Billions of phishing emails are sent every day, and all it takes is one successful attempt to cause significant harm. Don't expect email breach attacks to go away any time soon. Instead, take action to reduce your risk of being victimized.

What layers can you put in place to enhance email protection?

Educating your employees is an important first step. You can put different protection systems and security software solutions in place for the business, but human behavior will always be one of your biggest cyber-risk factors.

To protect your business from email breaches you'll want to:

- Train employees on the risks of email and password behavior
- Emphasize the importance of strong passwords and good cyber hygiene
- Foster a culture of compliance and individual responsibility for cybersecurity
- Institute an effective cybersecurity monitoring program to safeguard your business

Email security training tools exist that can train and test your employees on a frequency of your choosing (weekly, monthly, quarterly, etc.). These tools provide video training and multiple-choice testing, as well as credentialing, for the variety of email security topics that cybercriminals try to exploit and leverage (i.e., phishing, spoofing, etc.). Such tools can also be used to test employees' application of cyber training by launching simulated emails, using dummy email attacks, to see if individuals apply what they've learned in a real-life, but safe, email attack attempt scenario.

In addition, consider putting a **password manager application** in place to guide employees into setting more complicated passwords.

As we mentioned in an earlier chapter, multi-factor authentication (MFA) is a highly effective tool in protecting email accounts. MFA requires a second-level requirement for

authentication and access like a code sent over text to a mobile device, so that having a stolen email password isn't enough to gain access.

Limiting access to password-restricted systems and applications can curtail the damage if one user's credentials are exposed. Many applications allow restrictions on individual access so that users can access components of an application (enough to perform their work), but not have access to the entire application or all its data.

Lastly, ongoing monitoring of technology for signs of suspicious activity is a key safeguard. Automated alerts and the tracking of activity logs puts your business in a proactive stance against attacks, and significantly improves your odds of avoiding a disaster.

By creating a business environment that prioritizes detection and prevention, you reduce the risk of an email scam debilitating your business. With how widely used it is in all facets of a business, email is a common vulnerability hackers try to exploit to gain access to business networks and data. But you can safeguard yourself, your employees, and your business with the proper tools and training.

7

BEEF UP YOUR PROTECTION WITH ANTIVIRUS AND DETECTION RESPONSE SOFTWARE

Antivirus software is specially designed to identify, stop, and remove viruses or malware. It's one of the most commonly used cybersecurity tools by businesses of all sizes. You've probably heard the names of a few antivirus providers already: Norton, Kaspersky, Bitdefender, Windows Defender, McAfee.
Something is always better than nothing, and the same applies to free antivirus software that comes with a laptop or other devices. But new cyber threats emerge daily. An antivirus

software program will provide your business with proactive protection, so you can find peace of mind.

If you're ready to explore the next step past basic antivirus, consider investing in endpoint detection and response (EDR) software. EDR goes beyond prevention of specific malware and virus attacks, analyzing behaviors and activity on employees' devices to proactively identify where attacks may come from.

There are a variety of EDR programs available, and it's best to select one from a vendor that aligns with the rest of your company's software solutions. An EDR program follows a subscription model and is best for businesses looking to invest in a strong cybersecurity presence, including those who may be applying for cyber insurance.

Beyond EDR, businesses ready to make a heavy investment in antivirus protection set up what's called a managed detection and response (MDR) program. MDR is not just one piece of software, it's a set of systems that requires significant coordination of people and technology.

What are the estimated costs associated with each of these solutions? Let's take a look:

- ***Basic antivirus:*** $0-30 per month, per user
- ***EDR:*** $5-50 per month, per user
- ***MDR:*** High initial investment needed, plus continual investment in upgrades and personnel

8

THE IMPORTANCE OF BUSINESS CONTINUITY, DISASTER RECOVERY, AND BACKUPS

Being able to access and interpret data is crucial . But what happens if your business is hit by a natural disaster or cyberattack? That's where business continuity planning, disaster recovery planning, and data backup solutions come in. These are essential components of good cybersecurity practices, and they can help ensure that your business can continue to operate in the event of a disaster.

A business continuity plan (BCP) is a document that outlines how a business will continue to operate in the event of a disaster. It includes detailed plans for disaster recovery and data backup, as well as procedures for restoring operations. A BCP helps ensure that your business can continue to function in the event of a disaster, and it's essential for protecting your data and keeping your business running smoothly.

What are the components of a business continuity plan?

A good BCP will include the following:

- ***Risk Assessment:*** A good business continuity plan will include a risk assessment. This assessment will identify the potential risks that could affect the business, such as natural disasters, power outages, or cyberattacks. The assessment will also determine the likelihood of these risks occurring and their potential impact on the business.

- ***Business Impact Analysis:*** A business impact analysis (BIA) is another important element of a business continuity plan. This analysis will identify which operations are critical to the business and how long the business can function without them. The BIA will also help

to determine the resources that will be required to keep these critical operations running in the event of an interruption.

- ***Recovery Strategies:*** Once the risks and impacts have been identified, recovery strategies can be developed. These strategies will detail how the business will continue to operate in the event of an interruption. Recovery strategies should be designed to minimize the impact of an interruption on the business and its customers.

- ***Communications Plan:*** A communications plan is another essential element of the BCP. This will detail how information will be communicated to employees, customers, and other stakeholders in the event of an interruption. The communications plan should include procedures for contacting employees, providing updates to customers, and issuing public statements.

- ***Training and Testing:*** A good BCP should also include training and testing procedures. Employees should be trained on their roles and responsibilities in the event of an interruption. Additionally, the plan should be tested regularly to ensure that it is effective and up-to-date.

- ***Maintenance and Updates:*** Finally, a good business continuity plan should be maintained and updated on a regular basis. As new risks emerge, or as existing risks change, the plan should be updated to reflect these changes. Additionally, new technologies or processes may be implemented that could improve the effectiveness of the plan.

How is business continuity different from disaster recovery?

A business continuity plan (BCP) and a disaster recovery plan (DRP) are two essential components of good cybersecurity practices. However, there are some key differences between these two plans.

A business continuity plan is a document that outlines how a business will continue to operate in the event of a disaster. It includes detailed plans for disaster recovery and data backup, as well as procedures for restoring operations. A business continuity plan helps

ensure that your business can continue to function in the event of a disaster, and it's essential for protecting your data and keeping your business running smoothly.

A disaster recovery plan is designed to help you rebuild your business after a disaster has occurred. It includes detailed plans for recovering lost data and rebuilding IT systems. A disaster recovery plan can help you get your business back up and running quickly after a disaster has struck.

A quality disaster recovery plan will include:

- ***Recovery Point Objective (RPO):*** The RPO is the amount of data that you are willing to lose in the event of a disaster. It's important to select an RPO that is achievable and realistic, so you can be sure that your data will be recovered in a timely manner.

- ***Recovery Time Objective (RTO):*** The RTO is the amount of time that you are willing to wait for your business to recover from a disaster. It's important to set an RTO that is achievable and realistic, so you can be certain that your business will be up and running as soon as possible.

- ***Backups:*** Good disaster recovery plans include regular backups of all critical data. This data should be stored in a safe and secure location, so it can be easily accessed in the event of a disaster.

- ***Testing and Maintenance:*** Your disaster recovery plan should be tested regularly to ensure its effectiveness. Additionally, the plan should be updated on a regular basis to reflect any changes in your business or the risk landscape.

How are backups important to disaster recovery?

If your business loses data in a disaster, proactively updating a backup copy of that data can make it easier to restore operations. Without a backup, you could lose weeks or even months of data and business operations.

To put it directly, backups help you minimize the impact of a disaster. If you lose data in a disaster, you can easily restore it from your backup copy. This will help you get your business back up and running quickly and minimize the damage caused by the disaster.

In addition, backups are important for business continuity. In addition to helping you recover from a disaster, backups can also help you continue to operate in the event of an interruption. This can be critical for preserving your business data and ensuring that your customers are taken care of.

What's the urgency around business continuity and disaster recovery planning?

When it comes to the importance of having a BCP and a DRP in place, the data is motivating.

A study by the National Small Business Association found that:

- 43 percent of small businesses experience data loss every year
- 60 percent of small businesses that suffer a data loss are out of business within six months

These statistics make it clear: data loss can have a significant impact on a small business's bottom line.

With that being said, small businesses that have a DRP in place are more likely to recover from a data loss. A DRP can help you rebuild your business after a disaster has occurred. It includes detailed plans for recovering lost data and rebuilding IT systems, so that your business can get back up and running quickly after a disaster has struck.

Small businesses typically don't have the same resources as larger businesses to recover from a data loss or disaster. That's why it's essential for small businesses to develop a disaster recovery plan, a business continuity plan, and a data backup solution. These plans and solutions can help you protect your business data and keep your business running smoothly in the event of a disaster.

9

WHY AUTOMATED DATA BACKUPS STILL NEED MANAGEMENT

So, your business is backing up its data in case of cyberattack or other disastrous disruption. Good work! You can pat yourself on the back for that.

But don't get too complacent with your automated backup solution because automated backups still need monitoring and management.

Having decided to back up data, you should feel confident you can withstand an attack or recover from unexpected downtime. But your technology environment is constantly changing. And that constant change can affect the surety of your backup solution.

How can automated backup systems fail?

An IT technician can set an automated backup to run on a set schedule, and with a time selected that causes the least interruption while ensuring up-to-date data. But over time, things change within the technology environment being backed-up.

It's important to remember, unmanaged automated backups are set up for a company's technology configuration at the time they are installed. A lot can happen in the meantime as the company's IT environment evolves, such as:

- An unplugged backup device
- An altered device letter, which means the device isn't found
- Moved folders containing important data
- Software updates that might require changed backup settings
- New servers, devices, or applications not accounted for in the original backup
- Migration from on-prem to the cloud
- Insufficient capacity for the backup

Without any monitoring of your backup solution, important data could still be lost.

What can you do to ensure backups are protected?

Automating your backups is a smart move and will provide important data protection while saving your business time and money.

Go the last mile by monitoring your backups to ensure data integrity as your technology environment changes.

Your company's IT professional or an IT service provider can take a hands-on approach to your automated backups. If there is a failure, they can address the issue quickly and alert you of any bigger issues. As a bonus, they can even run data-restore drills, helping you to prepare for challenges such as ransomware attacks or accidental data deletion.

CONCLUSION

There's a lot to digest when it comes to cybersecurity! What happens when you have all of these tools, policies, and procedures in place, you might ask? Those responsible for technology in your organization can feel confident in the layers of protection put in place. Employees across your business can gain a better understanding of common threats and how they can work safely and effectively. And leadership can rest easy knowing that their business has been made safe from outside cyber threats to the best ability possible.

We hope that by understanding the broader scope of how you can protect your business, you feel prepared to take action. That's where our Cybersecurity Workbook for 2023 comes in to play! Get your copy now – and feel free to reach out to our team if you need any help along the way.

OUR CORE VALUES

In our cybersecurity work, and in all that we do, the Lighthouse team is guided by three core values.

The first core value is to **Follow the Golden Rule,** and treat others the way you would want to be treated.

The level of service we provide is the same we would hope for in return. We invest the time that's necessary to help our partners find the best solution. Our team is also generous with their time and their networks, making connections and sharing expertise however we can.

Second, you'll hear our team say **"Be a Lighthouse"** often.

Because to us, that phrase guides the work we do. It's all about helping people. We tell the stories of our company in the hopes they inspire others, and we share our light with the communities we serve to uplift and support everyone we touch.

And lastly, our third core value is **Light Up Those Around You.**

We want to bring positivity and joy to every interaction, however we can. We build trusting and friendly relationships. And we have the proof to back it up, with satisfied clients across Western New York and beyond, and more than 150 five-star reviews online for the world to see.

We're serious when we say our goal is to be the most inspiring technology partner in the communities we serve.

And we hope this conversation about cybersecurity has inspired new conversations that can benefit you and your business.

LHTservices.com

Seneca One Tower
1 West Seneca Street, Suite 2820
Buffalo, New York 14203
(716) 634-0509

LHTservices.com

Seneca One Tower
1 West Seneca Street, Suite 2820
Buffalo, New York 14203
(716) 634-0509