SMALL BUSINESS CYBERSECURITY CHECKLIST

By Tobi Sonubi

Contents

Small Business Cybersecurity Checklist

1. Introduction to Cybersecurity for Small Businesses

Small businesses, like larger organizations, have sensitive information that needs to be protected. Some examples of this are email threads between employees, customer invoices, banking account numbers, product specifications, and formulas. A direct attack can cost a small business money, time, reputation, and even survival. Employees and contractors who need to access sensitive information must have workflows designed to protect this information. The rest of this document details the basics of cybersecurity for small businesses and the steps to implement a solid, limited-budget cybersecurity program. Implementing a robust cybersecurity program is within reach for small and midsized businesses. Following this checklist will get it running with an acceptable amount of security controls in place. (Bartik et al.2020)

Why Small Businesses Need Cybersecurity One common misconception is that smaller businesses face minimal cybersecurity risks and are therefore not worth targeting. However, a significant percentage of cyberattacks are directed against small businesses. Increasingly, smaller businesses are getting hit not for the information they have, but because their systems house information or act as conduits to larger businesses that are really being targeted. In fact, the number of small businesses reporting cyberattacks has increased over the past three years. The average financial impact of cyberattacks on small businesses is substantial. The average cost in time wasted dealing with those attacks is significant – the equivalent of over five weeks of work. Now is the time for small and midsize businesses to take proactive cybersecurity measures to protect sensitive information. (Tam et al., 2021)

2. Importance of Cybersecurity for Small Businesses

Cybersecurity is critical to protecting your business from financial ruin. Cyber incidents can result in anything from temporary slowdowns to bankruptcy. When businesses suffer a cyber incident, they also face the prospect of negative PR. Businesses that fail to enact cybersecurity measures to protect their confidential data risk losing customer trust. Small businesses are hit by cyberattacks over 4,000 times a day (Kelley). It's important to take cybersecurity seriously. Compliance and data leaks have become essential for businesses.

In today's market, cybersecurity for small businesses is just as important as it is for large corporations. Taking a proactive stance on cybersecurity can offer your business competitive advantages and put you in compliance with a variety of frameworks that are critical for business operations. Cyber incidents are costly. The most recent research revealed that over 66% of consumers would no longer do business with a company following a data breach (Balkin, 2020). Financial loss was a consequence of 6 in 10 cyber incidents experienced by small businesses surveyed. Almost four in ten concluded that the breached firm had failed to protect their data. Of those respondents who terminated their relationship after experiencing a cyber incident, 70% said it was because the business seemed 'untrustworthy.'

3. Key Cybersecurity Threats for Small Businesses

There are a multitude of different potential cyber threats that businesses can face, and being aware of them is often the first necessary step that business owners have to take in order to defend their company from them. This is especially true for small businesses, which should exercise an abundance of caution in the digital age. Professional security can often be out of reach for small operations, but generally speaking, having this information at your disposal is already a good step in the right direction when it comes to tackling these cyber threats and is capable of insulating your business from a range of potential threats.

While cyber crime is estimated to cost the UK over £21 billion annually, it also carries significant emotional impact for victims. Among the most frequently cited cyber threats, malware ranks near the top, transmitting through email or via download or USB device. Malware is the term to umbrella a wide range of hostile or intrusive software. It has the ability to incapacitate or damage networks. An even more common cyber threat is the phishing attack, which can be pursued through socially engineered phone calls or emails. For most small businesses, ransomware is listed as a potential problem. It mainly infects a network when a user downloads a file that is disguised as something appealing and is able to lock up data, regardless of whether or not a data set has already been encrypted. Despite being on the lower end in terms of frequency, a data breach could still potentially incur the most severe consequences for an organization. The average cost for a data breach in 2018 was $3.5 million. This could affect how customers view participating businesses as well. (Button et al.2022)

3.1. Malware

Small businesses are often targeted by cyber criminals to deliver malware. Malware is a term for any type of harmful software created to infect and compromise an endpoint, which could be anything from an individual device to an entire network. Viruses, worms, spyware, and ransomware are all examples of malware. Malware can enter a system when a user opens an email containing an attachment, visits a website that uses an outdated browser, engages in instant messaging, or connects via a network. The presence of malware on your system may result in the loss of critical company information and damage to your system. It could even lead to data leaks, resulting in a lawsuit from a client or customer. You don't have to be a software engineer to stay safe from malware. One can be proactive and adopt everyday habits such as regularly updating software and operating systems, deleting suspicious emails, using complex passwords, double-checking website links before clicking on them, and updating antivirus software regularly.

Antivirus programs work to prevent malware from entering a system and can remove malware that has already infiltrated a system. Most reputable antivirus products offer a business version that works on individual devices or on networked office computers. In addition to using antivirus software, it is a good practice to train staff to be aware of the dangers of malware and to take steps to prevent any system from becoming infected. Beginning with the basics, staff training for new employees should cover the following topics: not clicking on links or opening files from unknown senders, not illegally downloading and sharing copyrighted material, not opening any files from emails from banks or any other organization that asks to update personal or company information, and ensuring that software with permissions to bypass system firewalls is not used for any company-related issues.

3.2. Phishing Attacks

One common attack small businesses should be aware of is called phishing. Phishing is a tactic used to trick individuals into giving away their sensitive or private information. Phishing can take many forms, including:

- Email: Fraudulent or deceptive emails designed to fool the recipient into providing sensitive information or trick them into installing malware on their system.
- SMiShing: A clear attempt to deceive and trick individuals into divulging their sensitive or private information.
- Spear Phishing: A more targeted form of phishing that presumes to be from a sender who is known by the receiver. The goal is to get the victim to reveal confidential information.

Phishing emails often carry ransomware and other malicious software. These infections may disrupt business operations, in many cases leading to significant financial loss and reputational damage. To recognize and combat phishing, inform your employees about this risk and impress upon them to approach any unfamiliar communication, file, or visitor with an abundance of caution. Encouraging skepticism is not out of place when it comes to your

IT security. Make it company policy to adopt a zero trust model towards unfamiliar digital assets, meaning don’t trust; verify anything out of the ordinary.

While there is no clear dividing line between high-frequency, high-severity risks and high-frequency, low-severity risks as they relate to small business cybersecurity, phishing is generally near the top of both lists. Provide your team with ongoing opportunities to learn to recognize it and respond to any and all suspicious communications they encounter. With an informed and cautious workforce, small businesses can decrease the risks associated with email-borne malware and phishing.

3.3. Ransomware

Ransomware is a particularly dangerous threat for small businesses because it can stop day-to-day work. Ransomware is a type of malicious software that encrypts a victim's data, making it inaccessible until a ransom payment is made. Ransomware encrypts files and documents on a victim's computer rather than compromising a data breach or stealing data. Because ransomware encrypts data, it's impossible to access the data until it's decrypted with a private key. It's common for ransomware criminals to demand payment in cryptocurrency. The prevalence and sophistication of ransomware attacks have only grown since the malware was invented.

A study provides an idea of the scale and nature of the problem. It found that 2,354 U.S.-based governments, healthcare facilities, and schools were targeted by ransomware in 2020. Estimates the overall cost to victims was $20 billion. This figure includes the cost of recovery and ransom, but also an estimation of the cost to the victims' clients and customers. The city of New Orleans reportedly paid more than $7 million after a ransomware attack in 2019. In addition to this, New Orleans incurred millions more as part of their recovery efforts. To protect against ransomware, take the following precautions: Establish a regular data backup schedule; Back up data to a remote location; Store backups on a separate device; Don't rely solely on automated systems for data backups; Regularly update software, including your operating system; Consider hiring a cybersecurity team; Train employees to recognize phishing emails; Document an incident response plan.

3.4. Data Breaches

When a small business does not employ data protection measures, it's only a matter of time before a data breach occurs. When that happens, any information stored within the breached system could either be held for ransom or sold on the black market to the highest bidder. Worse yet, some hackers even use the information to predict what a consumer does so that they can steal additional pertinent information for an even bigger payday. Small business data breaches are usually caused by either hackers or by accidental exposure, or both of these causes. By having data access controls and encryption in place, hackers are less likely to get in and look around. Making data more difficult for hackers to steal is the best way a small business can prevent against hacking.

When a small business undergoes a data breach, they can face legal consequences as well as have financial losses. Fines and regulatory citations for businesses that have a breach are often associated with not having strong enough data encryption or with not protecting their systems well enough against hacker activities. Furthermore, if information about a person is stolen in a small business's data breach, these people could all decide that they want to sue the business that allowed their information to be stolen. Small businesses should take seriously the issue of good cybersecurity to avoid these potential issues. Having a cybersecurity audit performed on your systems will help a small business uncover what steps will work best for them. But most importantly, training employees on the best ways to handle customer data is the best defense a small business can use against human error related to data breaches.

4. Establishing and Cultivating a Cybersecurity Mindset in Your Small Business

While a complete and comprehensive plan for cybersecurity is an absolute necessity and serves as a crucial starting point, it is equally important to ensure that all employees possess a profound understanding of why cybersecurity holds such immense significance. One incredibly effective method of achieving this is by educating the workforce through the sharing of captivating anecdotal examples that emphasize the gravity and implications of data breaches and malicious viruses. By presenting cautionary tales rather than inundating individuals with overwhelming statistics and potential consequences stemming from cybersecurity compromises, the message is more likely to resonate and create a lasting impact.

It is imperative to acknowledge that when employees fail to uphold and maintain a secure online environment, they not only compromise the safety of sensitive customer and proprietary data but also peril the long-term prosperity of the company itself, as well as the well-being of their fellow colleagues. To cultivate a culture of security within the organization, there are several pivotal measures that can be implemented.

One such measure involves leaders consistently highlighting cybersecurity-related events throughout the year to bolster the significance of security training. Moreover, on a monthly basis, employees should receive concise yet informative tips and guidance, intended to further foster their comprehension of cybersecurity matters and enhance their cyber hygiene practices while operating within the workplace.

To establish a solid foundation of protection, open and transparent communication between the IT department and all employees must be prioritized. Given that employees are already juggling multiple priorities at work and in their personal lives, maintaining an environment where they feel comfortable and supported while seeking guidance or reporting potential security risks is of utmost importance. The organization should ensure that all IT security policies are clearly articulated and easily comprehensible, with regular training sessions held annually to update and reinforce these policies.

Recognizing and commending exemplary security behavior that contributes to the mitigation of potential threats is another integral component of fostering a secure environment. Implementing various channels and methods for employees to report security incidents, tailored to their individual preferences and comfort levels, is crucial. Additionally, a system of spot awards should be implemented, rewarding employees who promptly report imminent and dangerous activities that, if left unaddressed, could result in harm to individuals.

While the provision of anonymous reporting mechanisms has proven to be advantageous, it should be noted that many employees prefer a level of confidentiality. Creating a reporting portal that ensures confidentiality without the involvement of management, email tracing, or internet tracking is an example of an effective and discrete reporting method.

Continual education and training for staff members are fundamental processes that should be integrated into the company's culture. All individuals within the organization should be empowered to actively participate in the collective effort to maintain a secure environment, both during work hours and in their personal lives. Recognizing and rewarding employees who report phishing scams, viruses, malware, and instances of inappropriate network usage further reinforces the importance of cybersecurity.

Comprehensive cybersecurity is a multifaceted endeavor that necessitates the participation and commitment of every member of the organization. By prioritizing the education and understanding of employees, cultivating open lines of communication, and recognizing exemplary security behavior, a culture of security can be established, ensuring the company's ongoing protection and the well-being of its workforce.

5. Essential Cybersecurity Policies and Procedures

Digital security is a significant concern for small business owners. Numerous attacks continue to be launched by cybercriminals, and professionals agree that these threats are only increasing in sophistication. The implementation of cybersecurity policies and procedures is one measure that can be taken to mitigate threats. Without formal guidance, human behavior will always be fallible. If left to their own devices, people will behave in the way that feels physically most comfortable. The best way to standardize and monitor behavior within your team is to provide a clear set of guidelines that everyone is expected to follow. Abiding by formalized policies can significantly reduce the person-driven vulnerabilities in your systems.

So, what policies should small businesses be formalizing and implementing? For a large company with a large cybersecurity budget, this list would be exhaustive. However, for small businesses, the most critical cybersecurity policies are as follows: Password Management, Remote Work, Acceptable Use Policy, Email Policy, Incident Response, Data Backup, Cybersecurity Policy Review Procedures. Hopefully, businesses have already established the basic framework for security; however, frequent review and evolution of these policies is also important as new threats emerge. Without continual adaptation, a policy is useless. Staff training in cybersecurity policy and procedures is a fantastic step to improve any policy's effectiveness. Providing appropriate training to the people who will use them and ingraining a policy through a comprehensive set of standard operating procedures backed by strategic training can reduce the vulnerabilities in your systems through human error exponentially.

5.1. Password Management Policy

Passwords are the main defense mechanism to protect digital assets or any information from unauthorized users in an organization. It is the first line of defense and a gateway to secure systems. Password strength and uniqueness are key principles of the cybersecurity discipline. Thus, strong and unique passwords are an essential part of good security practices and help protect sensitive information from being compromised. A good password policy specifies what is expected of the end users with respect to password use. This includes rules for creating strong passwords, rules for managing and changing passwords over time, and how to construct a good password. The following are some principles to consider when creating a strong password policy: - At least 8 alphabetic and numeric characters. - At least one lowercase and one uppercase letter should be included. - Should be changed after 6 months or changed frequently. - Avoid using personal information that can be easily gained by others as a password. - Prohibit employees from sharing passwords with coworkers. - Use a management system to securely store and manage passwords. - Develop an education program for your employees to discuss the reasons for these policies to reinforce the need for compliance with these policies. The risk of not following these two pieces of advice is that if an attacker gains access to the password database, they can easily crack the password and take over the account, which will cost dearly to the organization. The consequences of poor password policies are normally seen in a security breach, leading to financial impact as well as reputational risk for the organizations. So it is advised to maintain a strong password policy and keep the password safe and secure from unwanted access. It is better to avoid providing any security questions that directly relate to personal lives in activities like social media, blogs, office documents, etc. Keep that information confidential and personal. Medical or test results should be carefully saved and not publicly open to access.

5.2. Data Backup and Recovery Policy

Data backup policy also needs to highlight the organizational commitment to ensuring adequate and regular data backups. While backing up your organization's crucial information might be considered the most important part of your cybersecurity strategy, vital to the success of any information technology (IT) procedure is the ability to restore data. This policy assists medium and small businesses in defining what must be done to back up efficient regular data and implement data restoration capabilities. Data backups - Organizations must create and implement an efficient regular data backup process to minimize data loss and make data restoration possible. Backup frequency - A minimum of weekly complete backups will be done daily for critical systems, databases, and files. Incremental backups should be performed at least once every 24 hours. Recovery storage - Backed-up data will be stored offsite in the cloud or at a third-party, segregated storage location.

The purpose of a data backup and recovery policy is to protect data from loss that occurs as a result of system failures, software corruption, hardware failures, hacking, and unintentional or intentional data deletion, encryption, or unauthorized alteration. Data backups are a critical data protection tool and essential to business mission continuity. Regular backups can guard against the loss of data in the case of incidents such as ransomware, hardware faults, software failures, environmental influences, or any cyber assault that encrypts data. Best practice is to automate backups and include data retention, or the retention of different versions of the data, for several days so in the case of a ransomware assault the organization can go back to a version of the data prior to the attack. Periodic testing to demonstrate the ability to restore from backup is a crucial part of the backup process. Employees working on the backup must be trained in backup and restore best practices. Risks associated with backing up and restoring data with sufficient frequency include permanent loss of data, increased downtime, or inability to demonstrate data provenance in the event of an investigation.

6. Securing Your Network Infrastructure: Implementing Stronger Protection Measures and Devices

6. Securing Your Network and Devices

Network and Device Security

When you have a small business, the cost of a data breach is potentially catastrophic. Sixty percent of businesses shut down within six months of a cyber incident. That’s why, when it comes to the cybersecurity of your small business, you need to be proactive. Follow our guide to cyber protection with these six tips.

Defense in Layers/Edge Protection

Deploy firewalls to protect the perimeter of your network and segment your network with internal firewalls. Consider using a VPN to set up remote access to your network. Deploy an Intrusion Detection System or Intrusion Prevention System to protect traffic once it enters your network. If your business has a Wi-Fi network, provide separation between any guest networks and your internal network.

Antivirus software is still a critical component of protecting your business systems. Make sure to enable automatic updates and scans so the AV doesn’t slow down your users with full-system scans. Use Mobile Device Management to enforce a passcode, enable full-device encryption, and enable timeouts for device inactivity. If applicable, you can use apps like GPS, remote wipe, or remote lock in case a phone or tablet is lost or stolen. Inventory your business Internet-facing systems and services and ensure that they are secured in accordance with industry standards and best practices.

Regularly check and apply software updates and patches on all systems used in your business. This includes IoT devices, which have been the cause of several large global cybersecurity incidents in the past three years. Test your security with protocols such as penetration tests and security scanning tools regularly. Do an annual risk assessment. Once completed, implement strong assurance controls over the sensitive systems and data identified within the assessment. Continuously monitor software and end-user behaviors for malicious activity. Cybersecurity threats are always changing and evolving, so a continuous assessment of your current security posture is needed. Study and stick to industry best practices for all cybersecurity matters, including hardening Internet-facing services, firewall rule design, and data protection.

Regularly test, update, or assess your Disaster Recovery and Incident Response plans.

6.1. Firewalls and Intrusion Detection Systems

A firewall is a set of capabilities that prevents discretionary access between two or more networks. Firewalls can be used to protect both end-user systems and network servers. Firewalls establish a barrier between a trusted internal network and an untrusted external network. Firewalls can be installed on both external and internal networks. Several types of firewalls are used. Application-layer firewalls are considered the most powerful type of firewall because they can understand and interpret application data at all seven layers of the OSI model, without any blind spots. Ultimately, however, any type of firewall is better than none at all. Deciding which firewall to use is largely a matter of costs and benefits for small companies.

As an intrusion detection system, a firewall is typically a device or application that monitors system or network activities for malicious activities or policy violations and produces reports for management. Some systems may attempt to stop an intrusion attempt, but this is neither required nor expected when dealing with firewalls. A firewall's primary function is to stop malicious traffic, or at the very least slow it down, before it can reach your firewalls. A good firewall product is the first line of any computer security strategy. These typically are vendor-patched on a regular basis, and it is vital to keep these systems up to date with the latest security patches, which often enhance the firewall tools. Firewall logs should be regularly reviewed as well to check for issues or unusual activity. Lastly, small business computers should be periodically assessed for security issues at best.

6.2. Antivirus Software

Given the considerable risk of a cyber attack resulting in data loss or breach, every small business should prioritize cybersecurity. One of the key elements of a robust small business cybersecurity plan is antivirus software. Antivirus software, also known as anti-malware, is a tool or a set of tools used to detect and remove malware from a computer or network. There are two major components to any antivirus solution: an engine, which scans files for pattern-based threats, and a database of virus definitions, which are known patterns of malware. There are a few different types of antivirus solutions on the market, such as those that use signature-based detection, real-time analysis, or heuristics, which check code and file characteristics. Most of today's antivirus packages make use of multiple detection methods and update regularly in order to ensure that your business network is protected. Since cyber criminals develop and release new threats daily, antivirus software needs to be updated constantly in order to have any chance of keeping up. Neglect in updating antivirus software will significantly increase your business's risk of a data breach. The most advanced antivirus solutions use real-time views of the web, leveraging intelligence and automation. Advanced threat management can instantly quarantine and remove threats from any device identified as the source of the infection. When considering whether an antivirus solution is right for your business, take some time to become informed on how it works and how it would integrate into your unique system. Additionally, you may want to compare the various options available to you, including customizability, ease of use, and monthly or yearly subscription costs. Neglecting the inclusion of antivirus software in your cybersecurity strategy is primarily risky. Any data breach or other cyber attack will have costly ripple effects, not only in terms of direct financial expense, but also in relation to a tarnished business reputation that can make it difficult to recover. This likely seems like a high price to pay for something that can easily be avoided. Employee education is key. When it comes to securing your business through a cybersecurity plan, employee education is obviously quite important. By providing education and sharing the guidelines with employees as they are developed, you encourage them to be a proactive and involved component of your business's cybersecurity plan. This helps protect the company as a whole, not to mention the personal health of their own computer equipment. Make sure your employees understand the need for antivirus solutions; if, for any reason, they are not already using their own personal software. Employees also need to understand that, as mandated, all company software and hardware must be equipped with antivirus solutions. They cannot bypass company security. Best practices dictate using the stringent security policy settings available within a given antivirus package; employees cannot avoid scanning large files, updating virus definitions, or scanning removable media. Policy files that control company security can be found within the preference settings in an antivirus software program. Therefore, the antivirus policy cannot be easily overwritten or avoided by unauthorized users. Antivirus software plays a crucial role in safeguarding small businesses from cyber attacks. With the ever-growing threat landscape, it is imperative for businesses of all sizes to prioritize cybersecurity and implement robust measures to protect their data and networks. Antivirus software serves as a vital defense mechanism, detecting and eliminating malware that can compromise the integrity and security of computer systems. By scanning files for pattern-based threats and utilizing a comprehensive database of virus definitions, antivirus software effectively identifies and removes malicious software from computers and networks. Depending on the type of antivirus solution chosen, businesses can benefit from signature-based detection, real-time analysis, or heuristic scanning that analyzes code and file characteristics. In order to keep up with the rapidly evolving threat landscape, antivirus packages frequently update their detection methods to ensure continuous protection of business networks. These regular updates are crucial as cyber criminals develop and release new threats on a daily basis. Failing to update antivirus software significantly increases the risk of a data breach for businesses. Advanced antivirus solutions are equipped with real-time web views, leveraging intelligence and automation to instantly quarantine and remove threats originating from infected devices. When considering an antivirus solution for your business, it is important to thoroughly understand how it works and how it can seamlessly integrate into your existing system. It is also advisable to compare the different options available, taking into account factors such as customizability, ease of use, and subscription costs. Neglecting to include antivirus software as part of your cybersecurity strategy poses significant risks. Any data breach or cyber attack can have far-reaching consequences, not only in terms of financial losses but also reputation damage that can hinder business recovery. The potential costs associated with such incidents make it crucial for businesses to take proactive steps to protect their data and networks. Employee education is a key aspect of a comprehensive cybersecurity plan. By providing employees with the necessary education and guidelines, businesses can empower them to actively participate in safeguarding the company's cybersecurity. This not only protects the business as a whole but also ensures the personal well-being of employees' own computer equipment. Employees should understand the importance of antivirus solutions and, if they are not already using their own personal software, they should be encouraged to do so. It is essential that every staff member comprehends the company's policy mandating the use of antivirus software on all company-owned software and hardware. By adhering to strict security policy settings within the antivirus package, employees cannot bypass crucial security measures like scanning large files, updating virus definitions, or scanning removable media. The antivirus policy can be safeguarded within the preference settings of the software program, making it difficult for unauthorized users to override or avoid. With the ever-increasing threats of cyber attacks, businesses cannot underestimate the importance of antivirus software in their cybersecurity strategy. By investing in robust antivirus solutions and ensuring employee education, businesses can significantly mitigate the risk of data breaches and protect their valuable assets.

6.3. Mobile Device Management

Mobile devices are playing an increasingly prominent role in every aspect of our lives, including the professional world. More than 44% of employees use personal devices for work. When companies allow staff to switch between working on computers and personal mobile devices, small business owners create enormous security vulnerabilities. Mobile devices already represent significant cybersecurity risks because they are easy to misplace or steal, connect to non-secure networks, or get infected with malware. Allowing employees to use them to work from cafes, airport terminals, and anywhere else they can find a Wi-Fi signal only increases the danger. To combat these threats, many small businesses are implementing Mobile Device Management solutions.

A Mobile Device Management application allows business owners to manage and secure employees' mobile devices. MDM solutions offer a variety of helpful features, such as remote device wiping and location tracking. These give you the ability to respond quickly after you lose a device, as well as the ability to track down its location. Additionally, MDMs offer data encryption support, which means you can encrypt any data stored on an employee's device. This ensures that even if the device falls into the wrong hands, the data remains secure and protected. Furthermore, it is crucial to have a remote lock feature, as that can give an employee enough time to retrieve the lost item or even delete data manually to prevent unauthorized access.

In addition to utilizing MDM solutions, all mobile devices permitted on your company network should adhere to a comprehensive list of acceptable use guidelines. These guidelines should outline the expected behavior of employees when using their mobile devices for work purposes. Additionally, it is essential to emphasize the importance of using secure sockets layer (SSL) or transport layer security (TLS) to protect data in transit. By utilizing these encryption protocols, sensitive information transmitted between devices and networks is safeguarded from interception and unauthorized access.

Due to the possibility that many users may not comply with your company's policy, it is crucial to train your employees on best practices to ensure data security. Employees should be educated on the risks associated with connecting to public Wi-Fi networks and should be discouraged from using open hotspots without a secure password. Encouraging the use of virtual private networks (VPNs) when accessing sensitive data and communicating with company networks is also recommended. Regular audits of your MDM policy will also allow your company to test the efficiency of your management tools and adjust policies when necessary. This proactive approach ensures that your organization remains up-to-date with the latest security measures and can swiftly respond to any emerging threats.

To summarize, the increasing use of mobile devices in the professional world necessitates the implementation of robust security measures. Mobile Device Management solutions provide business owners with the necessary tools to manage and secure employees' devices, including remote wiping, location tracking, data encryption, and remote locking. Adhering to comprehensive acceptable use guidelines, utilizing SSL/TLS protocols, and providing employee training on data security best practices are also essential. Regular audits of your MDM policy allow for continuous improvement and adaptation to evolving security threats. By taking these precautions, small businesses can mitigate the risks associated with mobile device usage and protect their valuable data and assets.

7. Protecting Customer Data

Some of the most sensitive information small business owners handle is customer and user data, which can include everything from names and addresses to payment details and social security numbers. If your business experiences a breach, those details could be sold and used for fraud and identity theft, with potentially devastating consequences for your customers. In addition to scaring off existing customers, a data breach can generate negative press, decrease interest in your business from potential customers, and put you at risk for penalties and legal action. Make sure you've put these DIY cybersecurity practices in place at your small business.

- Ensure Customer Data Privacy

— Encrypt customer data from end to end, and make sure that your website encrypts data in transit. Regularly review functionality for data leaks, and only store credit card information if necessary.
— Limit who can access customer data to those who need to use it. User groups and permissions can help ensure that only staff members who have to handle sensitive data can access it.
— Many different countries have laws and regulations regarding data

privacy. Make sure you're aware of the rules and regulations that apply to your business to ensure IT compliance. Part of cybersecurity is earning your customers' trust by easing their fears about how you're handling their data. Document a data security plan and make it available for customer and client review on request. Ensure that your plan includes incident response procedures and system monitoring guidelines. There are many different frameworks and standards you can use to design a data security plan.

Evaluate Your IT Security Regularly — It's not enough to hire a single IT individual or to install a security suite and stop there. Evaluate your network security tools and monitoring processes and perform IT security risk assessments regularly to catch new and unforeseen IT threats. You should also install the latest security updates and patches for new software regularly. Commence an ongoing managed IT security assessment or monitoring service to ensure that when potential dangers surface, your IT security manpower is ready. Regular reevaluation can also catch problems, such as data stored improperly or an increase in security risk questions from new hires, before they become severe.

7.1. Data Encryption

In its simplest form, encryption is the process of encoding information in such a way that only authorized parties can access it and those who are unauthorized cannot. Through encryption, businesses can protect sensitive data, and it can be used to secure data both when it is at rest and when it is in transit. There are a number of methods for encrypting data and several industry standards for encryption that businesses can choose from. There are a number of best practices to think about when it comes to data encryption. For instance, if you have sensitive data stored in the cloud, you will want to ensure that your cloud provider encrypts data at rest and in transit. Additionally, you should incorporate encryption as part of your data management policies and practices. This can include training for employees on how and when to encrypt sensitive data. You should also look for the most up-to-date encryption algorithms and technologies, as this will help protect your data from increasingly sophisticated cybercrimes. This approach argues for employing data encryption strategies that are attuned to the size and capabilities of the small business, yet still consistent with general approaches to cybersecurity. It is recognized that there are potential difficulties in limiting protections to sensitive data. Employees may not be aware of what the sensitive data are, and in any case, any data about customers or suppliers are typically deemed sensitive, especially if they include Personally Identifiable Information. The next best practice, however, is to encrypt sensitive information, and the subsection will discuss that approach in detail, which can serve as a short to-do checklist for encrypting data. It is therefore recommended that every small business interested in avoiding a data loss incident or limited data loss incidents should immediately prioritize encrypting their sensitive data as much as possible. Everything stated above regarding adoption and implementation has the caveat that individual small businesses should consult with an IT professional who can help shepherd them through the process. It is best for the encryption process to be folded into a broader conversation about cybersecurity that includes considerations of access to various data architectures and network systems. This may involve authentication technologies and strategies, additional cloud-based or server-based security precautions, or more widespread deployment of encryption technologies. General cybersecurity awareness and workplace policies, on a continuing basis, should also educate employees on the necessity of encrypting data. Encryption is a crucial aspect of securing data and should be embraced by businesses of all sizes to protect their valuable information from unauthorized access and potential breaches. By implementing robust encryption methods, training employees on encryption practices, and staying updated on the latest encryption technologies, businesses can enhance their cybersecurity and safeguard sensitive data effectively. Considering the individual needs and resources of small businesses, it is important to devise encryption strategies that align with their capabilities while adhering to established cybersecurity principles. Encrypting sensitive information, especially data concerning customers and suppliers, is highly recommended to ensure the utmost data protection.

Small businesses should prioritize the encryption of their sensitive data to mitigate the risks of data loss incidents. However, it is crucial for small businesses to seek guidance from IT professionals to navigate the encryption process effectively. Integrating encryption into comprehensive cybersecurity discussions will enable businesses to address various aspects such as data architecture, network systems, and access controls. This may include implementing authentication technologies, additional security measures for cloud-based or server-based systems, and widespread deployment of encryption technologies. Maintaining a culture of cybersecurity awareness and regularly updating workplace policies will further reinforce the importance of data encryption among employees. By embracing encryption as a fundamental practice, businesses can bolster their security posture and safeguard their sensitive information in an evolving threat landscape.

7.2. Compliance with Regulations in Relation to Data Privacy Laws (e.g., General Data Protection Regulation, California Consumer Privacy Act)

Privacy and data protection are crucial components of laws and regulations in many countries and states around the world. These laws include various data protection acts that aim to safeguard personal information and ensure its secure handling. While smaller businesses may have some leniency in terms of regulatory requirements and the effort/cost involved in compliance, it is generally expected that all businesses adhere to the basic principles of data protection.

Compliance with data protection laws involves various obligations that businesses must fulfill as part of their daily operations. This includes prioritizing the security and confidentiality of customer data and implementing measures to protect it. Regulations require businesses to have a clear understanding of the information they collect, how it is used, who it is shared/sold to, and when it is deleted. Additionally, individuals have the right to access their own data and request modifications or deletion at any time.

Small business owners should be cautious not to make any false claims about data protection or privacy compliance. The penalties for misleading advertising can be severe and potentially more damaging than non-compliance itself. Demonstrating a genuine commitment to privacy and data protection can enhance a business's reputation and foster trust with customers and potential clients. By showcasing an understanding of individuals' rights and actively working towards regulatory compliance, businesses can establish themselves as trustworthy entities that prioritize privacy.

In the event that issues arise, whether inadvertently or otherwise, businesses that can demonstrate a history of due care and efforts to follow regulations can more effectively address and mitigate the problems. Consistently maintaining privacy measures and complying with data protection requirements is an essential aspect of ongoing business operations. This may involve regular audits to assess the effectiveness of established procedures and ensure compliance. Additionally, staff training is crucial to ensure that employees understand the importance of data privacy and are equipped to handle customer information appropriately. It is often recommended that businesses regularly train their employees on data privacy policies and discuss any updates or changes to operations and procedures. Staff members are often the weakest link in a data privacy system, so their awareness and adherence to guidelines are instrumental in maintaining a secure environment.

Regardless of the size or revenue of a business, conducting audits and implementing privacy measures is essential. Regular assessments can help identify any gaps in data storage systems or operational processes that need to be addressed. If you are a small business owner seeking to align your operations with laws and regulations, or if you need assistance in achieving compliance, please do not hesitate to reach out. Our team is here to support you and ensure that your business meets all necessary requirements for privacy and data protection.

8. Incident Response and Business Continuity Planning

Small businesses are an increasingly attractive target for cybersecurity incidents. This is why it is crucially important that all businesses, regardless of their size or industry, establish a comprehensive and well-defined incident response process to react effectively to a breach. An incident response plan serves as a roadmap, outlining the necessary steps to follow when dealing with a potential security incident, addressing different stages of incident handling, and detailing the specific roles and responsibilities of each individual involved in the process. The incident response process itself comprises several key components, each of which plays a critical role in ensuring the organization's ability to detect, respond to, and recover from a cybersecurity incident.

The first component of the incident response process is documentation. It is essential to document every aspect of the incident response, including the staff involved, their respective responsibilities, and the specific procedures to be followed. This documentation serves as a reference point and ensures consistency in the response efforts.

Another important aspect of the incident response process is incident identification and containment. This involves promptly identifying and isolating the affected systems or networks, preventing further damage and minimizing the impact of the incident. Timely detection and containment are crucial in preventing the incident from spreading and causing additional harm.

In addition to containment, incident response also involves the recovery of business processes. This entails restoring the affected systems, networks, and services to their normal and secure state, ensuring that the organization can resume its operations as quickly as possible.

An effective incident response process should be closely integrated with a business continuity plan. A business continuity plan outlines the strategies, procedures, and resources necessary to ensure the organization's ability to continue operating in the face of a disruption or breach. It should identify potential risks and vulnerabilities, enabling the organization to prepare and respond effectively. Different members of staff should be assigned to potentially vulnerable systems, ensuring that there is a clear understanding of their roles and responsibilities in the event of a breach.

Like incident response plans, business continuity plans should be regularly tested, updated, and communicated throughout the organization. Regular testing ensures that the plans are effective and that all staff members are familiar with their roles and responsibilities. Communication is vital in ensuring that everyone is aware of the plan and knows what actions to take in case of an incident.

It is crucial to emphasize that the effectiveness of incident response and business continuity plans depends on the company's overall culture of preparedness. This begins with educating and raising awareness among the executive team and board members about the potential severity and consequences of a data breach. Documenting these conversations and any action steps taken demonstrates proactive efforts and can be valuable evidence in the event of a lawsuit or regulatory inquiry.

While incident response focuses on individual security incidents, it is essential to understand that in the event of a breach, the organization may need to navigate multiple complex incidents simultaneously. This requires effective coordination and management to maintain the continuity of operations and prevent significant disruptions to the business.

In conclusion, small businesses must prioritize establishing a robust incident response process that includes comprehensive documentation, incident identification and containment, recovery of business processes, integration with a business continuity plan, regular testing and updating, communication, and fostering a culture of preparedness. By taking these proactive measures, businesses can effectively respond to cybersecurity incidents, minimize the impact, and maintain the security and continuity of their operations.

9. Vendor and Third-Party Risk Management

It is absolutely imperative to effectively manage the potential risks associated with vendors and third-party entities in the realm of small business cybersecurity. Partnering with vendors and engaging in third-party relationships can create vulnerable points of entry for malicious actors to infiltrate interconnected business networks. The scope of the IT environment becomes significantly broader when vendors are integrated into online systems or entrusted with the handling of data that flows between their own computers and those of the businesses they serve. If these connections are not adequately secured and diligently monitored, they can create additional avenues for attackers to exploit or introduce further vulnerabilities into the intricate ecosystem of business operations. Therefore, it is of utmost importance to take into account the risks posed by vendors and thoroughly evaluate your technology ecosystem as you navigate the following best practices:

- Thoroughly evaluate the security practices of potential third-party entities. When considering prospective vendor partners, it is crucial to initiate crucial conversations regarding cybersecurity. By identifying technology partners who share common standards and are committed to secure network connectivity, the task of building a robust and impenetrable network becomes substantially more feasible.

- Establish comprehensive security requirements. Once businesses have a comprehensive understanding of their cybersecurity status, it is advisable to commence the process of establishing unambiguous requirements and security considerations when engaging in contracts for new technology or services. These contractual agreements must clearly stipulate the responsibilities and obligations of both parties to ensure the mutual safeguarding of each other's interests. More detailed information pertaining to this foundational aspect of mutual acceptance was elaborated upon in previous discussions.

- Vigilantly monitor security practices. Small businesses should actively engage with their third-party partners to ensure that they have robust cybersecurity practices in place. It is crucial to thoroughly document the extent of their responsibility in terms of securing the solutions or services they provide. Regular and consistent communication is vital to ensure ongoing compliance and the sustained effectiveness of the established security measures.

To further bolster the defense against potential cyber threats stemming from vendor and third-party involvement, small businesses should consider the following additional practices:

- Implement regular and thorough risk assessments specifically focused on vendors and third-party entities. These assessments should evaluate the potential vulnerabilities that arise from the integration of vendors into the IT infrastructure. By conducting regular audits, businesses can identify any weaknesses or gaps in security protocols and take immediate action to rectify them.

- Establish strict protocols for vendor and third-party access to sensitive data. By implementing access control measures, businesses can ensure that only authorized personnel have the necessary permissions to access and handle sensitive data. This can include measures such as multi-factor authentication, encryption, and regular audits of access logs to detect any unauthorized access attempts.

- Continuously monitor vendor and third-party activities within the network. This involves implementing advanced monitoring solutions that can track and analyze network traffic to identify any suspicious or anomalous behavior. By carefully monitoring all network activities, businesses can quickly detect any signs of a potential security breach and take swift action to mitigate the risk.

- Regularly update and patch all vendor-provided software and systems. Vendors often release updates and patches to address security vulnerabilities in their software and systems. It is crucial for businesses to promptly install these updates to ensure that they have the latest security measures in place. By neglecting software updates, businesses leave themselves at greater risk of falling victim to cyber attacks.

- Establish a robust incident response plan that includes specific procedures for addressing security incidents involving vendors and third-party entities. This plan should outline the steps to be taken in the event of a breach or security incident and should include clear communication channels with vendors and third parties to coordinate response efforts. Regularly testing and reviewing the incident response plan will help ensure its effectiveness in real-world scenarios.

By following these expanded best practices, small businesses can significantly enhance their cybersecurity posture when it comes to managing the risks associated with vendors and third-party entities. Proactive evaluation, comprehensive security requirements, vigilant monitoring, risk assessments, strict access controls, continuous network monitoring, regular software updates, and a robust incident response plan are all crucial components of a holistic approach to small business cybersecurity in an increasingly interconnected digital landscape.

10. Regular Security Audits and Assessments

A security audit is an essential process that plays a crucial role in identifying any security vulnerabilities present in an information system. It serves as a fundamental component of an organization's security risk management program and should be conducted at regular intervals. The audit itself involves a thorough examination of the information system's policies, regulations, and associated documents, alongside a comprehensive review of the system protection policies and the overall implementation across the entire organization. By conducting these audits, various differential access points, protective gaps, and potential performance gaps can be identified and appropriately addressed.

Additionally, control security assessments are conducted to analyze potential security vulnerabilities that may exist within the control bias control mechanism of the information system. This assessment is also useful in identifying any deviations in system configurations that could potentially hinder the confidentiality, integrity, or availability of a data system. By conducting vulnerability assessments, both external and internal reviews of enterprise security controls are performed to ensure the ongoing support and maintenance of enterprise security. Various assessment techniques are commonly employed, such as penetration testing, internal drive-by scans, external perimeter scans, and distributed denial of service (DDoS) evaluations.

Moreover, internal audits or assessments are conducted to gauge the effectiveness of company security policies and standards, as well as the overall performance of certain approaches in the long run. These assessments encompass a comprehensive analysis of employee behavior and system functionality. In order to accomplish this, methods such as employee surveys are employed to evaluate the efficacy of their most recent security training. Additionally, database scanning, firewall rule evaluations, best practice reviews, and network-based scans are utilized to scrutinize the system's current state. The objective of these evaluations is to conduct regular system tests, thereby identifying any weaknesses or vulnerabilities that need to be addressed before they are exploited. This proactive approach ensures the continuous robustness and resilience of the information system.

Furthermore, organizations can collaborate with external security experts to conduct more extensive audits and assessments. These experts bring a wealth of knowledge and experience in identifying potential threats and vulnerabilities that may go unnoticed by internal teams. By leveraging their expertise, organizations can gain new insights and perspectives on their security posture, allowing them to make informed decisions and enhancements. External security audits often involve thorough penetration testing, advanced vulnerability scanning techniques, and in-depth analysis of security controls and practices. This collaborative effort between internal teams and external experts ensures a comprehensive assessment of the information system's security.

Moreover, as technology advances and new threats emerge, it is crucial for organizations to keep up with the evolving landscape of cybersecurity. Regular security audits and assessments play a vital role in adapting to these changes and ensuring that the information system remains secure against emerging cyber threats. By staying vigilant and proactive in identifying and addressing vulnerabilities, organizations can maintain the trust of their stakeholders, protect sensitive data, and prevent potential financial and reputational damages.

Security audits are an indispensable part of an organization's security risk management program. These comprehensive assessments help identify and address security vulnerabilities, ensuring the continuous robustness and resilience of the information system. By conducting regular audits, organizations can proactively mitigate risks, adapt to evolving cybersecurity threats, and maintain the trust and confidence of their stakeholders. With the collaboration of internal teams and external experts, organizations can leverage cutting-edge techniques and expertise to enhance their security posture and protect their valuable assets.

11. Cybersecurity Tools and Resources for Small Businesses

When it comes to professionals and small businesses, the idea of cybersecurity tools can feel extensive. They can roughly be split into three groups: tools that aim to block incoming threats, detect when a threat has made it onto your network, and respond to an attack. Here are a few examples:

- Password managers can help with blocking and detection, as they keep track of all the different secure logins and alert users to known breaches when they occur.

- Firewalls can prevent attacks from affecting your network, but require a team to set up and maintain.

- Security information and event management (SIEM) systems can detect threats on your network, but are significantly more costly than firewalls.

- Virtual private networks (VPN) and multi-factor authentication (MFA) might be a response to a threat, as they check the types of devices and people accessing a network and ensure access controls for them.

The most important thing to remember is that tools should be able to grow with your business - you shouldn't have to adapt your strategy to fit a tool. Moreover, tools that make sense for a large organization might not make sense for you, and there are lots of free and low-cost resources available if you have the time to look for them.

Organizations and resources can help you pay for tools and offer free advice or training. It's also good to look around and stay informed about the newest threats and tools that might become relevant if your business grows. Expanding your knowledge and understanding of cybersecurity tools is essential to protect your small business from potential threats and attacks. By familiarizing yourself with the various options available, you can select the tools that best suit your specific needs and requirements. Remember, investing in cybersecurity is a proactive step towards safeguarding your sensitive data, ensuring the trust of your customers, and maintaining the integrity of your business.

12. Sample Cybersecurity Checklist

This checklist is designed for small businesses or organizations to identify key cybersecurity practices and controls that are reasonable business practices to implement. This list is not exhaustive and should be periodically reviewed and updated. Each control is described in an actionable format.

Sample Cybersecurity Checklist

SECTION ID	Control	Description	Comments	Due Date	Assigned To	Status	Section Status
1. Scan Network Firewall and Update Security Subscriptions							Yes
1.1 Scan Network Firewall and Update Security Subscriptions	Review firewall rules: Regularly examine and update firewall rules to ensure proper network segmentation, traffic filtering, and protection against unauthorized access. Pay particular attention to rules governing Remote Desktop Protocol (RDP) traffic to specific servers or internal computers, and non-secure traffic to internal web servers or phone systems.	Check rules for RDP, internal traffic, etc.	Refer to Firewall Policy	2024-10-31	Network Administrator	YES	Yes
1.2 Scan Network Firewall and Update Security Subscriptions	Update security subscriptions: Ensure that your security subscriptions are current to maintain the effectiveness of your firewall and other security tools in inspecting incoming and outgoing traffic and blocking malicious activities. Regularly review and renew subscriptions as needed.	Ensure subscriptions are current	Review renewal dates	2025-01-01	Security Manager	YES	
2. Review User Accounts And Security Groups							No

2.1 Review User Accounts and Security Groups	Disable inactive user accounts: Periodically review user accounts to identify those that are no longer active or have been assigned to former employees. Disable these accounts to prevent unauthorized access.	Review and disable unused accounts	Review ongoing	2024-10-31	Security Administrator	NO	No
2.2 Review User Accounts And Security Groups	Review security groups:Regularly assess the permissions and access rights granted to security groups. Ensure that groups have appropriate levels of access to network resources and that membership is restricted to authorized users.	Ensure groups have appropriate permissions	Refer to Security Group Access Control List (ACL)	N/A	Security Administrator	YES	
3. Run Domain Name System (DNS) Lookup							Yes
3.1 Run Domain Name System (DNS) Lookup	Verify SPF record: Conduct a DNS lookup to confirm that your domain has a Sender Policy Framework (SPF) record in place. An SPF record helps prevent spoofing attacks, where malicious actors attempt to send emails that appear to originate from your domain.	Confirm SPF record is in place	Review DNS records	2024-10-31	Network Administrator	YES	Yes
4. Activate Group Policy Lockout							No

4.1 Activate Group Policy Lockout	Enable account lockout policy: Configure your Group Policy settings to lock out user accounts after a specified number of failed login attempts within a given time period. This helps deter brute-force attacks and unauthorized access.	Set lockout policy for failed login attempts	Review policy settings	2024-10-31	Security Administrator	NO	No
5. Two-factor Authentication (2FA)							No
5.1 Two-factor Authentication (2FA)	Enable 2FA for email: Implement two-factor authentication for all email accounts to add an extra layer of security and prevent unauthorized access. Consider using a strong authentication app or hardware token in addition to a password	Use 2FA for email accounts (if supported)	Enabled for Office 365	2024-10-31	IT Helpdesk	YES	No
5. 2Two-factor Authentication (2FA)	Enable 2FA for online accounts: Review your online accounts and enable two-factor authentication for any that support it, such as social media platforms, banking portals, and cloud storage services. This helps protect your accounts from unauthorized access, even if your password is compromised.	Enable 2FA for other supported online accounts	Review and enable where available	2024-11-15	IT Helpdesk	NO	
Section 6: Replace Vulnerable Software/Hardware							No

Section 61 Replace Vulnerable Software/Hardware	Review vulnerable software: Regularly assess your network for vulnerabilities, including outdated software, weak configurations, and known security flaws. Use vulnerability scanning tools to identify potential risks. Patch and update all software components to address known vulnerabilities and security holes. Prioritize critical updates and patches.	Identify outdated or unsupported software	Review and update inventory	2024-11-15	IT Operations	NO	No
Section 6.2 Replace Vulnerable Software/Hardware	Replace unsupported hardware: Identify hardware components that are no longer supported by the manufacturer and pose a security risk. Develop a plan to replace outdated hardware with supported models	Replace hardware without security patches	Assess hardware lifecycle	2024-12-31	IT Operations	NO	
Section 7: Activate BitLocker							Yes

Section 7.1 Activate BitLocker	Enable BitLocker: Utilize BitLocker to encrypt your Windows drives, protecting sensitive data from unauthorized access even if the device is lost or stolen. This is particularly important for laptops and other portable devices	Encrypt Windows drives	Enabled on critical systems	2024-10-31	IT Operations	YES	Yes
Section 7.2 Activate BitLocker	Backup recovery keys: Store BitLocker recovery keys securely and in multiple locations to prevent data loss in case the encryption key is forgotten or inaccessible. Consider using cloud-based storage or a physical backup	Store recovery keys securely	Backups stored in secure location	2024-10-31	IT Operations	YES	
Section 8: Data Backup							No
Section 8.1 Data Backup	Implement automatic backup: Establish a comprehensive backup schedule to ensure that critical data is regularly backed up to prevent data loss in case of system failures, cyberattacks, or other incidents.	Configure automated backups	Daily backups scheduled	2024-10-31	IT Operations	YES	No

Section 8.2 Data Backup	Perform regular restores: Regularly test your backup procedures to verify that data can be restored successfully. This includes restoring test data sets and verifying data integrity.	Test backup integrity	Restore tests conducted quarterly	2024-12-31	IT Operations	NO	
Section 8.3 Data Backup	Encrypt backup data: Protect sensitive data in backups by using encryption to prevent unauthorized access. Choose a strong encryption algorithm and securely manage encryption keys.	Protect sensitive data in backups	Encryption enabled	2024-10-31	IT Operations	YES	
Section 8.4 Data Backup	Store backups off-site: Ensure redundancy and disaster recovery by storing backups in a location physically separate from your primary data center or office. This helps protect against data loss in case of fire, natural disasters, or other catastrophic events.	Ensure redundancy and disaster recovery	Off-site backups sent to cloud storage	2024-10-31	IT Operations	YES	
Section 9: Install Endpoint Security Software							Yes

Section 9.1 Install Endpoint Security Software	Deploy endpoint security: Install a robust endpoint security solution on all devices to protect against malware, viruses, ransomware, and other cyber threats. Choose a solution that includes antivirus, anti-spyware, firewall, and intrusion prevention capabilities.	Install business-grade endpoint protection	Endpoint security software deployed	2024-10-31	IT Operations	YES	Yes
Section 9.2 Install Endpoint Security Software	Update endpoint security: Keep endpoint security software up to date with the latest virus definitions, patches, and security updates to ensure maximum protection. Enable automatic updates to minimize the risk of vulnerabilities.	Keep software up to date	Automatic updates enabled	2024-10-31	IT Operations	YES	
Section 10: Security Awareness Training and Testing							No
Section 10.1 Security Awareness Training and Testing	Conduct security training: Provide ongoing security awareness training to employees to educate them about common cyber threats, best practices for safe online behavior, and how to recognize and report suspicious activity.	Provide regular training to employees	Annual training sessions scheduled	2024-11-15	HR	YES	No

Section 10.2 Security Awareness Training and Testing	Conduct security testing: Evaluate employee awareness through simulated phishing attacks or other testing methods. This helps identify knowledge gaps and areas for improvement in security training.	Evaluate employee awareness	Phishing simulations conducted quarterly	2024-12-31	Security Manager	NO	
Section 11: Establish and Enforce Password Policy							Yes
Section 11.1 Establish and Enforce Password Policy	Review and reset weak passwords: Regularly review user passwords and reset any that are weak, easily guessable, or reused. Encourage employees to use strong, unique passwords.	Ensure strong passwords are used	Password policy enforced	2024-10-31	IT Helpdesk	YES	Yes
Section 11.2 Establish and Enforce Password Policy	Enforce password complexity: Implement a password policy that requires strong passwords with a combination of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information like names or birthdays.	Require strong password requirements	Password policy includes complexity rules	2024-10-31	IT Helpdesk	YES	

Section 11.3 Establish and Enforce Password Policy	Implement password rotation: Require employees to change their passwords periodically to prevent unauthorized access in case their passwords are compromised. Set a reasonable rotation schedule, such as every 90 days.	Force periodic password changes	Annual password resets required	2024-12-31	IT Helpdesk	YES	

References:

Bartik, A., Cullen, Z., Glaeser, E. L., Luca, M., Stanton, C., & Sunderam, A. (2020). The targeting and impact of paycheck protection program loans to small businesses. NBER Working Paper, (w27623). github.io

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. Computers & Security. [PDF]

Kelley, P. T. (). Evolution of Cyber Attacks and Their Economic Impact (2022). scholar.archive.org. archive.org

Balkin, J. M. (2020). The fiduciary model of privacy. Harv. L. Rev. F.. yale.edu

Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. Criminology & Criminal Justice, 17488958221128128. port.ac.uk