INTELLIGENT
TECHNICAL SOLUTIONS

THE ULTIMATE GUIDE TO CYBERSECURITY FOR SMALL BUSINESS OWNERS

If your business uses the internet, it doesn't matter how small your company is; you need cybersecurity. It's no longer optional. In fact, small to midsize businesses (SMBs) are more likely targets for cybercriminals looking to make a quick buck. That's because larger organizations tend to have better security measures and policies in place compared to their smaller counterparts.

It all boils down to resources. Large enterprises have more time, money, and resources to deploy top-of-the-line security. Smaller organizations often don't have the same capabilities. However, that doesn't mean your cybersecurity goals are dead in the water. There are ways for SMBs like yours to implement robust security measures to protect data, assets, and customers. However, you must invest your resources in solutions that make the most impact - a task that's easier said than done.

Intelligent Technical Solutions (ITS) has been helping small businesses bolster their cybersecurity efforts for over two decades. In this guide, we will provide you with some practical and actionable tips on improving your cybersecurity as a small business owner. We will cover the following topics:

- Why cybersecurity matters for small businesses
- How to assess your cybersecurity risks and needs
- How to implement the essential cybersecurity tools and practices
- How to train your employees on cybersecurity awareness
- How to respond to and recover from a cyber incident

WHY CYBERSECURITY MATTERS FOR SMALL BUSINESSES

Cybersecurity is the practice of protecting digital assets such as data, systems, and networks from unauthorized access, use, or damage.

It matters for small businesses because:

Cyberattacks can cause significant financial losses.

According to a study by IBM, the average data breach cost for organizations with fewer than 500 employees is $3.31 million; the average cost per breached record is $164. That includes direct costs, such as remediation, legal fees, and fines, and indirect costs, such as lost revenue, customer churn, and reputational damage.

Cyberattacks can disrupt your business operations.

Cyberattacks can compromise your systems and networks, making them unavailable or unusable for a long time. According to the same IBM study, identifying a data breach takes 204 days on average, while trying to contain it can take up to 73 days. That downtime can significantly affect your productivity, customer service, and delivery of goods and services.

Cyberattacks can expose your customer data.

Cyber attackers can steal or leak customer data, such as personal information, payment details, or transaction records. This can violate your customers' privacy and expose them to identity theft, fraud, or other harm. This can also damage your customer trust and loyalty, which are essential for small businesses.

Cyberattacks can harm your reputation and brand.

Cyberattacks can tarnish your reputation and brand image in the eyes of your customers, partners, suppliers, regulators, and competitors. For a small business on its way up, that can cause significant damage. It can negatively impact your market share, growth potential, and competitive edge.

6 STEPS TO ASSESS YOUR CYBERSECURITY RISKS AND NEEDS

Knowing how dangerous an unprotected network can be, you might feel compelled to rush implementing cybersecurity measures. While we admit that time is essential, we urge you to take the time to assess your cybersecurity risks and needs properly. That will help you identify the most critical assets to protect, the most likely threats to face, and the most suitable solutions to adopt.

To assess your cybersecurity risks and needs, you can follow these steps:

Step 1: Inventory your assets

List all your essential assets for your business operations and customer service. These may include:

- Hardware (such as computers, servers, and routers)
- Software (such as applications and databases)
- Data (such as customer information)
- Networks (such as internet connection)
- Devices (such as smartphones)
- Cloud services (such as email)

Step 2: Identify your threats

Analyze the potential sources of cyberattacks that could target your assets. These may include external actors (such as hackers and criminals), internal actors (such as employees), or environmental factors (such as natural disasters). Consider the motivation, capability, and opportunity of each threat actor.

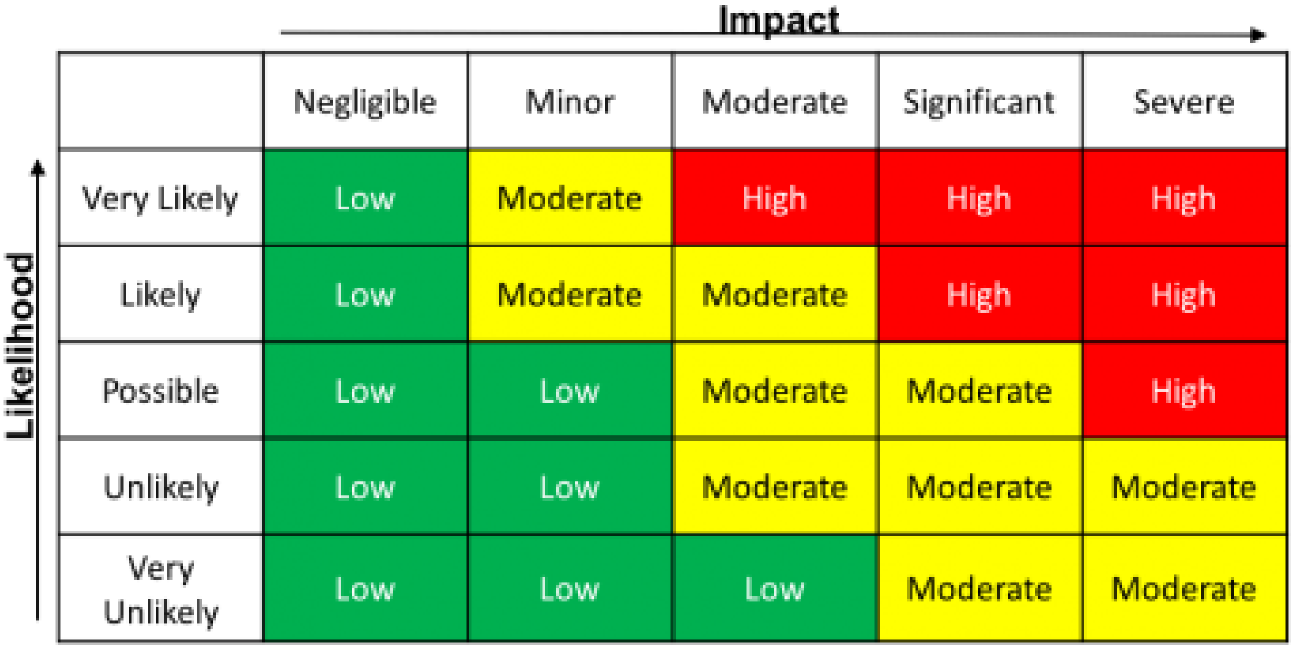
Step 3: Evaluate your vulnerabilities

Examine the weaknesses or gaps in your current security posture that threat actors could exploit. These may include:

- Outdated systems or software
- Lack of encryption or backups
- Weak passwords or authentication
- Insufficient policies or procedures
- Human errors or negligence

Step 4: Prioritize your risks

Estimate the likelihood and impact of each risk scenario that could result from a threat exploiting a vulnerability. Use a risk matrix to rank your risks from high to low based on their severity and urgency.



Impact

Likelihood

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate

Risk matrix sample

Step 5: Define your goals

Determine the desired outcomes of your cybersecurity efforts based on your business objectives and customer expectations. These may include:

- Preventing or reducing cyberattacks
- Complying with regulations or standards
- Enhancing customer trust or satisfaction

Step 6: Choose your solutions

Select the appropriate cybersecurity tools and practices to help you achieve your goals and address your risks. These may include:

- Technical solutions (such as antivirus, firewall, and encryption)
- Organizational solutions (such as policies, procedures, and training)
- External solutions (such as outsourcing, insurance)

10 ESSENTIAL CYBERSECURITY TOOLS AND PRACTICES TO IMPLEMENT FOR YOUR SMALL BUSINESS

Many cybersecurity tools and practices are available for small businesses, but not all are equally effective or relevant to your specific needs. To help you choose the best ones for your situation, we have compiled a list of the essential cybersecurity tools and practices that every small business should implement.

1. Endpoint Protection

Endpoint protection is software that protects your devices (such as computers and smartphones) from malware, ransomware, phishing, and other cyber threats. It can also monitor and control your devices' activity and access on your network. You should install endpoint protection on all your devices and update it regularly.

2. Firewall or Next-Generation Firewall (NGFW)

A firewall is a hardware or software that filters your network's incoming and outgoing traffic. It can block or allow traffic based on predefined rules or criteria, protecting your network from unauthorized or malicious access.

If you have the resources, an NGFW is the next evolutionary step for firewalls. NGFWs have the features of traditional firewalls but with added features to address a greater variety of organizational needs and block more potential threats. They combine a conventional firewall with other network device filtering functions, such as an application firewall using in-line deep packet inspection and an intrusion prevention system.

3. Data Encryption

Data Encryption is a process that converts your data into an unreadable format that can only be decrypted with a key. Encryption can protect your data from being stolen or tampered with while in transit or at rest. That is typically done automatically through software that encrypts your data on your devices, networks, cloud services, and email.

4. Backup

Backup is the process of copying your data to another location or medium that can be restored in case of loss or damage. Backups can protect your data from accidental deletion, corruption, ransomware, or natural disasters. It's crucial to back up your data, test the backups regularly, and store them in a secure and separate location.

5. Multi-Factor Authentication (MFA)

MFA is a method that requires two or more factors to verify your identity before granting access to your accounts or systems. These factors may include something you know (such as a password), something you have (such as a phone), or something you are (such as a fingerprint). MFA can prevent unauthorized access to your accounts or systems even if your password is compromised.

6. Virtual Private Network (VPN) or Zero Trust Network Access (ZTNA)

A VPN is a service that creates a secure and encrypted connection between your device and a remote server. It can protect your online privacy and security by hiding your IP address and location, encrypting your data, and bypassing geo-restrictions. You should use a VPN when connecting to public or untrusted Wi-Fi networks or accessing sensitive information online.

A better alternative to VPNs is Zero Trust Network Access (ZTNA). Unlike VPNs, which provide direct tunneled access to an endpoint, ZTNA solutions are founded on the principle of "never trust; always verify." That means they continuously verify that all users and devices trying to access resources in your network are who they say they are. Not to mention, they restrict access only to explicitly authorized resources and resource groups rather than the entire network.

7. Patch Management

Patch management refers to the practice of regularly patching your software. Vendors often create these patches and fixes to address security vulnerabilities or bugs in their products. Doing that consistently can prevent hackers from exploiting known flaws and vulnerabilities in your systems or software. As a general rule of thumb, you should install them as soon as they are available for all your systems and software.

8. Strong Security Policies

Security policies are documents that define the rules and guidelines for the use and management of your IT resources and data. Security policies can establish the roles and responsibilities of your employees, customers, partners, and vendors regarding cybersecurity. You should create and enforce security policies for all aspects of your IT environment, such as access control, password management, incident response, etc.

9. Regular Vulnerability Scan

Regular vulnerability scans refer to the process of evaluating the effectiveness and compliance of your cybersecurity measures against established standards or best practices. These assessments can identify the strengths and weaknesses of your security posture and provide recommendations for improvement. You should conduct vulnerability scans regularly or whenever there is a significant change in your IT environment.

10. Security Awareness Training

It doesn’t matter the size of your business; employees who lack security awareness are the biggest threat to your cybersecurity. That’s why security awareness training is crucial to any cybersecurity strategy. It empowers your team with the knowledge and skills to effectively recognize and respond to potential security threats. By fostering a culture of security awareness, even small businesses can significantly enhance their overall cybersecurity posture.

4 STEPS TO TRAIN YOUR EMPLOYEES ON CYBERSECURITY AWARENESS

Your employees are not only one of the most critical assets of your business but also one of the most vulnerable ones when it comes to cybersecurity. That's because cyberattacks rely on human interaction to succeed. Training your employees in cybersecurity awareness is crucial for preventing or reducing cybersecurity incidents.

To train your employees on cybersecurity awareness, you can follow these steps:

Step 1: Assess Their Knowledge and Behavior

Before you design and deliver any training program, you need to assess your employees' current level of knowledge and behavior regarding cybersecurity. You can use surveys, quizzes, tests, simulations, or interviews to measure their awareness, attitude, skills, and habits.

Step 2: Define Their Learning Objectives and Outcomes

Based on the assessment results, you must define each employee group or role's specific learning objectives and outcomes. These may include increasing their awareness of cyber threats, improving their skills in using security tools, and changing their habits in following security policies.

Step 3: Design and Deliver Engaging Content

Based on the learning objectives and outcomes, you must design and deliver engaging content covering the relevant topics and scenarios for each employee group or role. You can use various formats and methods, such as videos, games, stories, case studies, etc., to make the content more interesting and interactive.

Step 4: Evaluate and Improve Their Learning Outcomes

After you deliver the training program, you need to evaluate and improve the learning outcomes of your employees. You can use surveys, quizzes, tests, simulations, or interviews to measure their satisfaction, knowledge, skills, and behavior. You can also use feedback and analytics to identify gaps and areas for improvement.
To train your employees on cybersecurity awareness, you can use some of the following strategies:

- Use online platforms or services that can help you create and deliver engaging and interactive content for cybersecurity awareness training.
- Use gamification or incentives to motivate and reward employees for completing the training and passing the tests.
- Use metrics or feedback to evaluate the effectiveness of the training and identify areas for improvement.

HOW TO RESPOND TO AND RECOVER FROM A SECURITY INCIDENT

Despite your best efforts, you may still experience a cyber incident that affects your business. A security incident is any event that compromises the confidentiality, integrity, or availability of your IT resources or data. That can range from a minor annoyance, such as a spam email, to a major crisis, such as a ransomware attack.

How you respond to and recover from a security incident can make a big difference in minimizing its impact and restoring your everyday operations. To respond to and recover from a cyber incident, you can follow these steps:

Step 1: Activate your Incident Response Plan (IRP)

Your IRP is your action plan before, during, and after a cyber incident. It should include roles and responsibilities, communication channels, escalation procedures, contingency plans, and recovery steps. You should activate your IRP as soon as you detect or suspect a cyber incident and follow its guidelines.

Step 2: Contain the Incident

The first priority is to contain and prevent the incident from spreading or causing more damage. This may involve isolating or disconnecting the affected systems or devices, blocking or filtering the malicious traffic or activity, and changing or resetting the passwords or keys.

Step 3: Analyze the Incident

The next step is to analyze the incident and determine its scope, source, nature, and impact. This may involve collecting and preserving evidence, such as logs, files, and screenshots, identifying the indicators of compromise (IoCs), such as IP addresses, domains, and hashes, tracing the attack vector and timeline, assessing the data loss or exposure.

Step 4: Eradicate the Incident

The third step is eradicating the incident and removing any traces or remnants from your systems or devices. This may involve deleting or restoring the malicious files or programs, repairing or replacing the corrupted or damaged components, and updating or patching the vulnerable systems or software.

Step 5: Recover from the Incident

The final step is to recover from the incident and resume normal operations. This may involve restoring your data from backups, testing your systems or devices for functionality and security, and notifying your customers or partners of any issues or actions taken.

To respond to and recover from a cyber incident, you can use some of the following strategies:

- Use cloud-based or managed solutions that provide rapid and reliable recovery capabilities.
- Use artificial intelligence or machine learning techniques to help you detect and analyze incidents faster and more accurately.
- Use incident response plans or teams that can help you contain and recover from incidents promptly and effectively.

READY TO BOLSTER CYBERSECURITY FOR YOUR SMALL BUSINESS?

Cybersecurity is not only a concern for large corporations and government agencies. Small businesses are also vulnerable to cyberattacks that can compromise their data, reputation, and operations.

However, cybersecurity is not optional for small businesses; it's a necessity. By investing in cybersecurity, small businesses can protect their assets, customers, and reputation from cyber threats. They can also gain trust and loyalty from their customers and partners.

If you need help bolstering your cybersecurity, schedule a meeting with one of our experts. ITS has helped hundreds of small businesses devise and implement robust security solutions that fit their needs.

Intelligent Technical Solutions
(885) 204-8823
www.itsasap.com