THE ULTIMATE CYBERSECURITY CHECKLIST FOR SMALL BUSINESS

Network security is no longer just a bonus — it's a requirement for every modern business. Data breaches and hacks can be extremely destructive, no matter the size of your business. If you're part of a small or midsize business, you may not have access to all the security options a bigger company has. This means you must prioritize security features you have access to and learn how to protect your company's data. Learn what you need to know with this small business cybersecurity guide:

Why Your Small Business Needs to Have a Plan

With cyberattacks of all kinds on the rise, it's important for your business to have a security plan. Sixty percent of small businesses that suffer a cyberattack are out of business in six months. Following cybersecurity tips for small businesses can help you avoid that consequence and others, such as:

Increasing Cyberattacks

During the pandemic, the proportion of new methods and malware used in cyberattacks rose 35%. Cyberattackers have more opportunities to infiltrate systems now that more employees are working from home on unsecured devices or networks. Companies are spread thin as people work from all over the globe. This leaves businesses vulnerable to hackers. Even though cyberattacks have always been a serious threat, your business may be at risk more now than ever.

Cybersecurity and Employees

Employees may not be educated about cyberthreats and can end up making a security mistake. This could be anything from clicking a link in a phishing email or not creating a strong enough password. This is always a threat regardless of company size and traditional security measures. Employee training must be part of a cybersecurity plan.

Damage Caused by Cyber Hacks

If you don't think cyber hacks could cause your business a lot of damage, you're mistaken. Even small businesses can be destroyed by cyberattacks and phishing. Criminals can steal your business data, financial data or hijack your applications.

It's not just your data that can be leaked, but your customers' and clients' data as well. If credit card or personal information is compromised, you'll be open to lawsuits and fines. Important data can also be blocked by hackers, and the only way to get it back is to pay a large ransom. A plan can maintain your business's reputation and customer base and save you from operation-halting ransomware attacks.

Why Small Businesses Are Vulnerable to Cyberattacks

Cybersecurity is critical for businesses of all sizes, but small businesses are typically more vulnerable to attacks. About 43% of cyberattacks are against small businesses. While small businesses may seem like they would be less of a target, that doesn't decrease the number of attacks. Small businesses are generally less protected, so hackers target them because it's easier.

Threats Not Taken Seriously

Many small business owners do not think they are at risk for a cyberattack. Many think there is no reason for them to be a target, so they don't even realize that hacking could be a threat. Because of this, they often don't invest any time or resources in preventing a cyberattack. This leaves their data vulnerable and easy to compromise. This also means they I will not be likely to detect a breach if it happens.

Lack of Security

Small businesses that choose not to invest resources will have a lack of security. This problem is so consistent that hackers target small businesses for this reason alone, with 42% of small businesses having no cyberattack response plan.

Even businesses that have some security typically hand off the required duties to someone with little to no experience in the field. This gives hackers an easy opportunity to steal your data. Even if the employee discovers a problem, it's likely they will not know what to do next.

Small Business Cybersecurity Checklist

Preventing cyberattacks is a critical part of your business. When you decide to implement or enhance security, you'll need to know where to start. Create a cybersecurity policy for your small business with these steps:

1. Expect a Breach

The best way to prepare for a cyber crisis is to expect one. Consider what data your company holds that is the most important and start there. This could be your services, website or payment information. Perform a risk assessment and determine where the holes in your security exist. Consider where a threat could come from and what you'll need to do if it happens.

2. Train Employees in Security Principles

Employees need to be aware of the part they play in keeping the company's data safe and secure. Educate your employees on the best ways to protect customer information and business data. Basic security practices include strong passwords and careful internet usage. Employees should also be aware of phishing scams and how to avoid them.

Cyberattacks are constant risks, so the training needs to be enforced and regularly reviewed. Annual training is a start, but your organization will benefit from two to three trainings a year.

Your company's security principles should be easy to find and consistently brought to your employees' attention. One example of this is to send out a company-wide email every time there is a phishing attempt or email scam that may have been sent to employees. This will help educate employees on what these security risks can look like.

3. Utilize Email Restrictions

Cybercriminals often use email to trick employees into clicking on malicious links. While training employees in security principles can help reduce the likelihood of employees clicking phishing links, there are other ways to help reduce the risk. Message encryption and antivirus software can help prevent threats. Spam filters can also prevent email scams from reaching their intended target.

4. Evaluate Your IT Security Resources

Consider the resources you already have available and what your options are. If you already have security measures in place, evaluate their usefulness and if they will really be sufficient if there is a cyberattack. Discover any weak points. Then, you'll have to do some research to determine what resources you may need to become properly protected. Identity and access management (IAM) is a crucial security resource your business may need.

If your business uses third parties to transfer any information, you should also evaluate any weaknesses they may have. Determine the information that is shared and make sure they are only receiving the information they need.

5. Establish an Internal Incident Response Plan

In the event of an attack, an incident response plan is critical in resolving the issue before it gets worse. You absolutely need a response plan to have a chance at defending your company from the dangerous effects of a hack. This internal incident response plan should contain guidelines on how to detect, respond to and recover from any data breach or network security issue.

There are some industry-standard response frameworks that provide a great start for your specific incident response plan. Try to be as detailed as possible so you can respond quickly without having to stop to think of what to do next. Any delay could leave your data vulnerable.

NIST Incident Response Plan Framework
The National Institute of Standards and Technology (NIST) framework includes:

1. Preparation
2. Detection and analysis
3. Containment, eradication and recovery
4. Post-incident activity

SANS Incident Response Plan Framework
The SysAdmin, Audit, Network and Security (SANS) framework includes:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned

These frameworks should be added to and modified to best fit your business.

6. Create a Mobile Device Action Plan

People often use their mobile devices to access work resources, and this can be a security issue. Mobile phones often connect to public networks, and they don't have a lot of security. Connecting to unsecured Wi-Fi can expose the device's data. Downloading malicious apps or opening spam emails or texts can also allow hackers to steal sensitive data.

Employees who use mobile phones for work should be required to:

- Password-protect their devices
- Encrypt their data
- Use a security app to prevent cyber hacks

Lost and stolen devices are also a major risk. Data can easily be compromised when a lost or stolen device ends up in the wrong hands. Create a reporting procedure for these devices and a plan of what to do next. In the event that an employee's device is lost or stolen, one of the first steps should be disabling that employee's passwords and access to company data.

7. Limit Employee Access and Authority

Access to company computers and data should be controlled. Employees shouldn't have access to data they don't need. Each employee should have a separate user account and only have the privileges they require to perform their duties.

Separate user accounts will make it much easier to identify user activity and data modification. One employee shouldn't have access to all systems — you should divide those responsibilities and permissions. And employees should not be able to install any software without permission.

Those measures keep some systems intact in case an employee's password is hacked or their data is otherwise compromised. In some cases, disgruntled employees could sell data from the company. This is just one reason why limiting permissions is in the company's best interest.

8. Install Firewalls and Anti-Malware Software

Both firewalls and anti-malware software help protect your business from threats:

- Firewalls are programs that protect your private network from being accessed by unauthorized users.
- Hardware firewalls protect your entire network from data breaches and malware.
- Software firewalls can only protect the device running the software.
- Anti-malware software offers defense against the malware that may make it through the firewall and other security measures.

These protections should be in place for every device and network your business uses.

This step can be difficult for companies that have employees who work from home. Employees' home networks should be protected by a firewall, and any device they use to access work resources should be protected with anti-malware software.

9. Implement Secure Data Retention Policies

Data retention is the collection, storage and management of data and information. A data retention policy contains the protocols for how long data will be kept, where the data will be stored and how the data will be removed. This is important because some data needs to be kept for legal reasons, but too much data can overwhelm the system. Deleting or moving old data can help free up storage space.

There are a few requirements in the United States, but the legislation is broken up into a collection of laws. These acts all have sections that pertain to data retention:

- The Federal Trade Commission Act
- Fair Labor Standards Act
- Bank Secrecy Act
- Health Insurance Portability and Accountability Act
- Federal Information Security Modernization Act
- Electronic Communications Privacy Act

There are also a number of industry-specific requirements you may be subject to. You'll have to review all the data you collect and determine what requirements apply to what data.

Classify each category of data and determine what type of data it is, where it should be stored, how long it should be retained and who can move, modify or delete it. Creating these policies will remove any questions when it comes to cleaning up storage.

10. Control Facility, Device and Network Access

It's important to prevent unauthorized individuals from accessing data with measures like these:

- Computers should be password protected and locked up when unattended.
- Employees should use strong, unique passwords for every account.
- Passwords should be reset regularly and after every potential breach.
- Your wireless access point or router should have the network name hidden.

Employees should use multi-factor authentication wherever possible.

Multi-factor authentication is an authentication method that requires each user to utilize different verification factors to gain access. Typically, users will be required to type the password and then enter a secret code that was sent to the verified phone number on file. This strategy greatly decreases the likelihood of a successful hack.

11. Create Backup Copies of Company Data

In the event of an attack or software malfunction, you'll need backups of your data. Backup data such as documents, spreadsheets, databases and accounting information on a regular basis. Automatic backups can help free up time, but data should be backed up at least weekly. This can be very time-consuming when done manually. The data copies should be stored offsite or in the cloud.

Your company website should also have backups. Check with your website manager or provider to ensure there are regular backups of website data. If your website is hacked, you will lose a significant amount of money to the recovery of your assets in addition to the costs that come with a data breach.

Having several copies of data that are kept safe in various locations will ensure your information is protected in case of an emergency. It allows you to recover your data in the event of a cyberattack, virus or natural disaster. Without data backups, you risk losing all your data and being unable to ever recover it.

12. Employ Best Practices on Payment Cards

To protect payment information, you need to work with trusted processors and take precautions. There are three elements to consider:

- **Fraud management:** Only allow payment methods that have buyer identification verification and a high reputation for preventing fraud. The employees who are taking payments need to be trained on the rules and regulations so they can avoid leaving the company vulnerable to fraud.
- **Security:** Billing address information should match the IP address, data should be encrypted, payment information should be tokenized and strong customer authentication should be used. Your payment gateway should have built-in fraud monitoring. Additionally, employees should not be able to use personal cell phones while in a work area in which payments are taken. Mobile devices can easily record audio or take pictures of sensitive financial data that could be exploited.
- **Compliance:** There are also privacy and security standards you need to comply with. The Payment Card Industry Data Security Standard (PCI DSS) works to guard sensitive payment data. There are 12 requirements to follow under PCI DSS, broken down into areas like maintaining a secure network and protecting cardholder information. You need to create a program for vulnerability management that you regularly monitor and make an information security policy. Your company should also have access control measures for employees.

13. Upgrade Your Company's IAM

Identity and access management or IAM, consists of the business processes that control electronic identities. Operating with inefficient or outdated identity and access management systems puts you at a higher risk of hacks and data breaches. There are several benefits of IAM systems:

- Enhanced security
- Fewer password issues
- Improved user experience
- Reduced IT costs

An IAM system allows you to keep track of employee activity, control access, detect suspicious activity and automate other user account processes. Identity and access management makes managing identities, authentication and authorization an easy and automated task. This saves you time and money while increasing the security of your business.