10-Step Cybersecurity Plan for Your Small Business

Cybercriminals target businesses of all industries and sizes. According to a study conducted by the Better Business Bureau, 42% of small businesses have been the targets of cyberattacks.

Almost all cyber-attacks are intended to obtain personal data to use in identify theft. While larger organizations store much more information to steal, small businesses have less secure networks, making it easier to breach the network.

It's important to protect your business from cyberattacks, but some business owners aren't quite sure how. Implementing cybersecurity basics and putting them in practice will help you protect your business and reduce the risk of a cyber-attack. Insurance carriers also require you to provide evidence that you're taking steps to protect your information.

To help you assess the efficiency of your current business cybersecurity practices, here's a 10-step plan to help you navigate through the world of cyber threats.

1. Inform your employees about your cybersecurity policies.

Set up IT cybersecurity practices and policies for your employees. This includes requiring strong passwords and establishing appropriate Internet usage guidelines that comprehensively discuss your business cybersecurity policies.

2. Update your software.

Cybercriminals can enter your computer network through outdated apps with known vulnerabilities. Make sure you regularly install software updates and patches for applications and operating systems as soon as they're available.

3. Place a firewall.

One of the first lines of defense in a cyberattack is a sturdy firewall. We recommend that all small to medium-sized businesses set up a firewall to create a barrier between your data and cybercriminals. Installing internal firewalls is also an effective practice to provide additional protection.

4. Back up all your data regularly.

Always back up all your business data including data stored in the cloud. To have the latest backup, check your on-premises systems, and cloud systems regularly to ensure that they are functioning correctly. Backup standards have evolved and protecting your data in all locations needs to be considered for you to be in a secure business position.

5. Secure your wi-fi networks.

Make sure your wi-fi network is secured, encrypted, and hidden. To hide your wi-fi network, set up your router so it does not broadcast the network name, and protect its access with unique identity access or a strong password.

6. Install anti-malware software.

Anyone can be a victim of data breach, no matter how vigilant one is. Since phishing attacks center on installing malware on the employee's computer, it's imperative to have anti-malware software installed on all devices and in your network.

7. Make an action plan for mobile devices.

Mobile devices can also impose cybersecurity threats, more so if they store confidential business data. It is best to require all employees to protect their devices with passwords, install security apps, and encrypt their data. In addition, establish protocols for reporting lost or stolen company equipment to the appropriate organizations and authorities.

8. Implement strong data protection procedures.

Running your office machines on the latest software, web browsers and operating systems are the best defense against cybersecurity threats. Devise and follow a business data protection strategy that encompasses strong security measures centered around the restriction of access.

9. Use strong passwords.

Basically, strong passwords are a complex combination of special characters, numbers, and letters that provides more security for all your online accounts. Require all employees to always use two-factor authentication when accessing sensitive business data. It's also best to encourage them to never disclose their usernames to third parties.

10. Restrict authority for software installations.

Employees should have limited access to all data systems and software installations. Any installation should only cater to their role's specific needs, and under the permission of the network administrator.

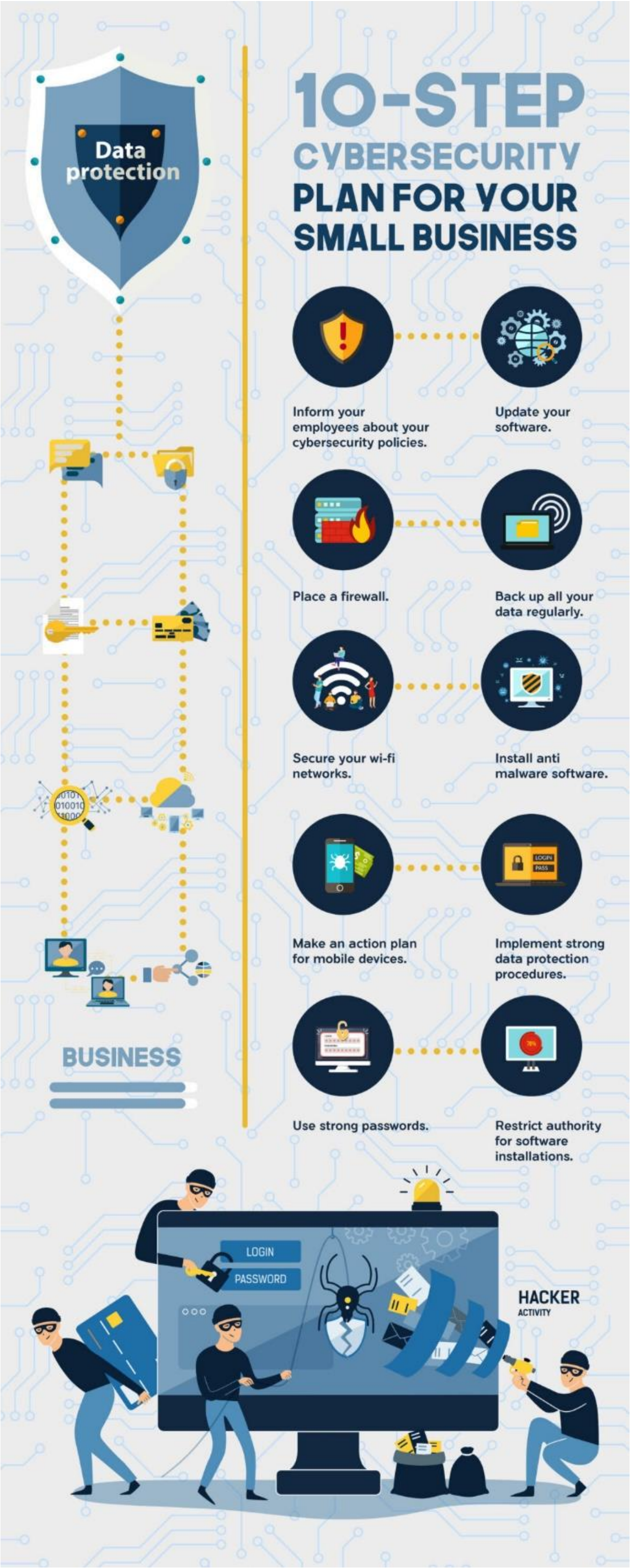
-

Your business cybersecurity is a moving target, and these cybercriminals become more advanced every day. To help you stay on top of the latest when it comes to cyberattacks and innovations on prevention technology, seek assistance from a dependable IT Managed Services Provider.

Phone: 209-573-3636

User & Device Security Essentials

- ➢ Identity Management & Security
  - ✓ Core Directory Services (Users & Groups)
  - ✓ Multifactor Authentication
  - ✓ Authenticator App
- ➢ Device Management & Security
  - ✓ Management Agent (Windows, Mac, Linux)
  - ✓ Data Encryption
  - ✓ Remote Lock & Erase
  - ✓ Remote Assistance
- ➢ Mobile Device Management & Security
  - ✓ Management Agent (Windows, Android, iOS)
  - ✓ Company Owned or BYOD (Bring Your Own Device) Management
  - ✓ Zero-Touch Enrollment
  - ✓ Remote Lock & Erase


Data protection
10-STEP
CYBERSECURITY
PLAN FOR YOUR
SMALL BUSINESS
Inform your employees about your cybersecurity policies.
Update your software.
Place a firewall.
Back up all your data regularly.
Secure your wi-fi networks.
Install anti malware software.
Make an action plan for mobile devices.
Implement strong data protection procedures.
Use strong passwords.
Restrict authority for software installations.
BUSINESS
LOGIN
PASSWORD
HACKER
ACTIVITY

Starting at

$14 per user monthly

If you have any questions, our contact information is:
Email: info@sparkmytech.com

PCI DSS Council - Reasons for PCI Compliance Status

PCI DSS is one example of why security and compliance is real and needed in your business. If you're processing credit card or electronic financial transactions, you must be PCI Compliant.

The following 12 reasons for passing or failing PCI compliance are listed below. Note the service is compliant with the requirements in the PCI ASV Program Guide.

1. CVSS base score of 4.0 or greater results in an automatic failure.

With a few exceptions, a vulnerability with a CVSS Base score of 4.0 or higher results in automatic failure. The service imports CVSS scores from the NIST database. For vulnerabilities that do not have a CVE, the service assigns its own CVSS score.

2. Un-supported software results in an automatic failure.

The service determines the version of the software and operating system running on the target machine. If it is an older version that is no longer supported by the vendor, that would result in an automatic failure.

On an ongoing basis, many new exploits and vulnerabilities are discovered for operating systems and security patches are released to address these security issues. It is important to apply software patches as soon as possible to protect operating systems against exploits and vulnerabilities.

3. Open access to databases results in an automatic failure.

The service detects open access to databases from the Internet. This configuration is a violation of PCI DSS section 1.3.7, and will result in an automatic failure.

On an ongoing basis, new vulnerabilities and exploits are discovered for databases and security patches are released to address these security issues. It is important to apply the patches as soon as possible to protect databases against exploits and vulnerabilities.

4. Built-in or default accounts results in an automatic failure.

The service will test and report on built-in or default accounts in routers, firewalls, operating systems, web servers, database servers, applications, POS systems, or other components. Any such vulnerability will result in an automatic failure.

Hardware and software vendors use built-in or default accounts and passwords to allow customers to log in to their products for the first time. Some of these accounts have no password at all; others have a password pre-defined by the vendor. These default accounts and passwords are well known in hacker communities, making systems vulnerable to attack. These accounts need to be assigned strong passwords or they should be disabled to protect systems with cardholder data.

5. Unrestricted DNS zone transfer results in an automatic failure.

The service will detect presence of a DNS server and detect known vulnerabilities and configuration issues, including unrestricted DNS zone transfer. Unrestricted DNS zone transfer will result in an automatic failure.

DNS servers resolve Internet addresses by translating domain names into IP addresses. Merchants storing cardholder data may have their own DNS server or one hosted by their ISP. If a DNS server is vulnerable, attackers can collect cardholder data by masquerading as the merchant's or service provider's web page. It is important to detect DNS servers and detect known vulnerabilities and configuration issues to protect cardholder data.

6. SQL injection vulnerability results in an automatic failure.

The presence of web application servers must be detected and any SQL injection vulnerability on these servers must be detected. Malicious individuals frequently exploit web application vulnerabilities to gain access to internal databases that potentially store cardholder data.

An SQL injection is a code injection technique that is used to exploit a security vulnerability in a web site's software. When exploited, SQL commands are injected from the web form into the database of an application to change the database content or dump the database information like credit card data or passwords to the attacker. It is important to detect SQL injection vulnerabilities so attackers do not gain access to internal databases that store cardholder data.

7. Cross-site scripting vulnerability results in an automatic failure.

The presence of web application servers must be detected and any cross-site scripting vulnerability on these servers must be detected. Malicious individuals frequently exploit web application vulnerabilities to gain access to internal databases that potentially store cardholder data.

Cross-site scripting is a type of security vulnerability found in web applications. When these vulnerabilities are exploited client-side script can be injected into web pages viewed by other users. These vulnerabilities allow attackers to bypass access controls such as the same origin policy. It is important to detect cross-site scripting vulnerabilities so attackers do not gain access to internal databases that store cardholder data.

8. Directory traversal on a web server results in an automatic failure.

The presence of web application servers must be detected and any directory traversal on these servers must be detected. Malicious individuals frequently exploit web application vulnerabilities to gain access to internal databases that potentially store cardholder data.

A directory traversal (or path traversal) exploits insufficient security validation or sanitization of user-supplied input file names. Upon successful exploitation characters representing "traverse to parent directory" are passed to the file APIs. It is important to detect directory traversal since this type of attack exploits a lack of web application security. This makes cardholder data and systems storing it vulnerable to attacks.

9. HTTP response splitting or header injection results in an automatic failure.

The presence of web application servers must be detected and any HTTP response splitting or header injection vulnerability flows on these servers must be detected. Malicious individuals frequently exploit web application vulnerabilities to gain access to internal databases that potentially store cardholder data.

HTTP response splitting is a web application vulnerability resulting from the failure of the application or its environment to properly sanitize input values. Header injection is a web application vulnerability that occurs when HTTP headers are dynamically generated based on user input. These vulnerabilities can be exploited to perform cross-site scripting attacks and other exploits. It is important to detect HTTP response splitting or header injection since his type of attack exploits a lack of web application security. This makes cardholder data and systems storing it vulnerable to attacks.

10. Backdoor applications, malware, rootkits or Trojan horse programs result in an automatic failure.

The service will detect and report well-known, remotely detectable backdoor applications installed on the servers. The presence of any such malware, including rootkits, backdoors, or Trojan horse programs will lead to an automatic failure.

A backdoor is a malicious software application, often commonly known in hacker communities. This malicious software needs to be identified and eliminated due to the risk backdoor applications pose to systems storing cardholder data.

11. Components with SSL version 2.0 or older result in a failure. SSL v3.0/TLS v1.0 with 128-bit encryption in conjunction with SSL v2.0 will also result in a failure.

Any component will result in an automatic failure if that component supports SSL version 2.0 or older OR if that component supports SSL v3.0/TLS v1.0 with 128-bit encryption in conjunction with SSL v2.0 due to the risk of forced downgrade attacks.

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of message transmission on the Internet. The Transport Layer Security (TLS), which is based on SSL, is a protocol that ensures privacy between communicating applications and their users on the Internet. There are well-known vulnerabilities that are easily exploitable, affecting SSL 2.0 and earlier. These security issues allow for interception or modification of encrypted data during transit. Also there are other vulnerabilities, referred to as forced downgrade attacks, which can trick an unsuspecting client into downgrading to a less secure SSL v2.0 in certain conditions. PCI DSS requirements state that strong cryptography and security protocols must be deployed and SSL v2.0/TLS v1.0 is the minimum standard due to the risk of forced downgrade attacks.

12. Vulnerabilities that are purely denial of service issues will not result in an automatic failure.

A denial-of-service vulnerability must not be ranked as a failure, per the guidance of the PCI Council.