SORCETEK
TECHNOLOGY GROUP

FIFTEEN-POINT

Cybersecurity Checklist

FOR TEXAS SMALL BUSINESSES

Table of Contents

The Rise of Cyber Attacks

Small businesses face many challenges in our technology driven world, not the least of which is cybersecurity.

While the digital landscape offers small businesses advanced tools for increased efficiency, along with greater opportunity to reach more customers and clients, it also means an increase in vulnerabilities and potential harm to your organization.

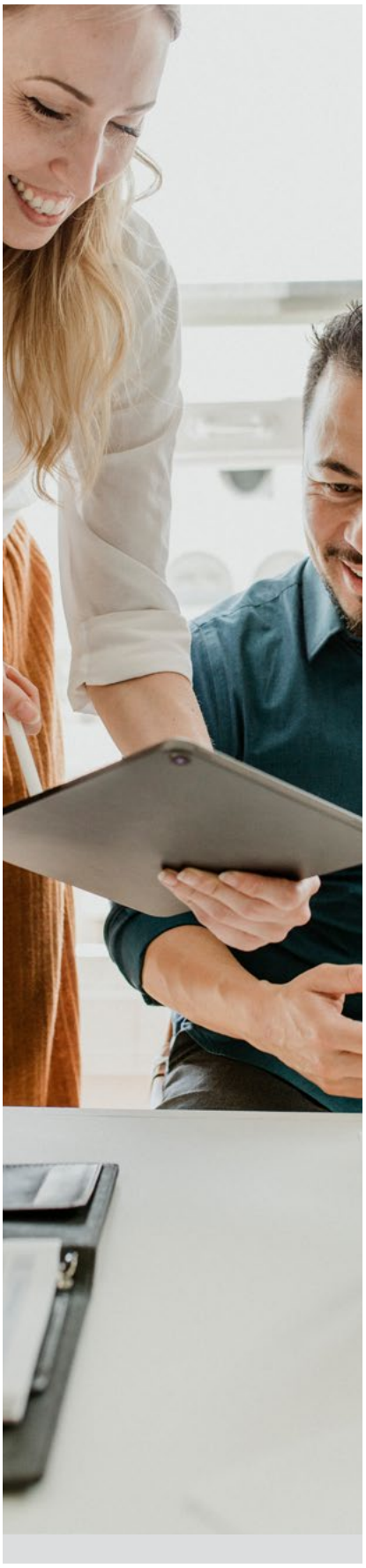
In fact, 43% of cyber attacks target small businesses, and only **14% are prepared to defend themselves.**

Further, 60% of those smaller companies who were attacked **did not survive past the next six months.**

Cyber attacks are usually financially motivated, but they don't just put monetary assets at risk. Private information, data loss, work disruption, compliance issues, trust and your reputation can all be compromised.

Fortunately, there are significant ways to stay ahead of cyber criminals. **Our fifteen-point checklist is a beginning guide to get you started.**

Fifteen-Point Checklist for Texas Small Businesses



01. Schedule Security Training

Your employees are your greatest asset and your most valued partners, but when it comes to cybersecurity, human error is the biggest threat. Basic security policies, practices and procedures need to be clearly and regularly communicated to all employees. Utilizing everything from structured lessons to role-playing to unannounced social engineering simulations will give you and your employees an edge against bad actors.

02. Avoid Phishing Scams

Phishing emails are one of the most widespread social engineering attacks used by cyber criminals. The recipient can be fooled into sharing sensitive company data or clicking on malicious links leading to even greater security breaches. Train your employees to recognize the signs of all types including **spear phishing, whale phishing**, phone **vishing** and text message **smishing**.

03. Install Antivirus Protection

The latest security software is one of the best safeguards against an attack. It's important to find the software that fits your particular industry and organization's needs, and that it comes from a known and trustworthy source. Make sure to run a scan using your security software after any updates, and always install updates as they become available.

04. Backup Your Files Regularly

Having a second copy of everything is essential. Understanding the ins and outs of traditional backups through an external hard drive versus backing up through the Cloud is important in deciding what's best for your business. The ability to regularly or, better yet, automatically back up documents, databases, accounting, financial and human resource files should all be considered.

05. Prioritize Risk Management

With effective management, comes prevention. Evaluating your assets and their vulnerabilities throughout your entire technology system is vital when it comes to preventing a cyber attack. This includes attack gateways on your hardware, software, applications and mobile devices. Analyze the risk and potential impact of different types of attacks so you can prioritize your security measures.

06. Use Two-Factor or Multi-Factor Authentication

Cyber criminals are more sophisticated than ever. Single sign-on (SSO) that utilizes just a username and password has become obsolete. Instead, implement authentication that requires two or more identifying credentials such as a password and temporary code when accessing applications and sensitive information.

07. Keep Software Up-to-Date

Seems easy, right? But with so many users in a business it can become a struggle and a hassle to stay on top of. Make sure your employees know to always activate software updates as they become available. Updates add new features, fix bugs and upgrade security. Consider a designated day of the week for everyone to update to the newest and safest versions available.

08. Keep Hardware Up-to-Date

Older and outdated hardware cannot support the latest software updates, putting your company at risk. In the case of a cyber attack, older hardwares responses and response time can put you at greater risk of damage.

09. Opt for a VPN

To privatize your network and increase security, use a virtual private network (VPN) to encrypt your connections and protect sensitive information. All of your employees should install the same, vetted brand of VPN. Utilize it if your organization has no internal network and anytime working at home or remotely.

10. Don't Use Public Wi-Fi

Public Wi-Fi networks are akin to computer hackers shooting fish in a barrel. Any information you send or receive on a public network is vulnerable even on a highly protected device. Instead, consider investing in a portable 4G hotspot for employees.

11. Use Strong Passwords and a Password Management Tool

Make passwords strong, never use the same one twice and change them at least once a year. To make it even easier to manage passwords, a password management tool or password account vault like LastPass is a reputable option for encrypting and locking up passwords so only you have access.

12. Stay Current with Cybersecurity Trends

Cyber criminals are always coming up with new and more sophisticated tactics to use in an attack. This means that it's important to stay on top of the latest in IT security. As new information is learned, make sure to continually update your employees through cybersecurity training sessions. For real-time cyber security news, follow us on Linkedin and Facebook.

13. Have a Mobile Device Action Plan

Mobile devices are one of the easiest gateways for hackers. On top of this, more and more employees are using laptops and phones to do work in and out of the office. Require users to password-protect their devices, install security apps and encrypt data.

14. Invest in Physical Security

Safeguarding your hardware, software, networks and data from burglary and natural disaster is also essential. Security systems, video surveillance, fire and flood protections are all items that need to be considered in protecting your business.

15. Utilize Secure File-Sharing

Your files are particularly at risk when in transit. To lessen the chance of them being co-opted by cyber criminals and to prevent unauthorized access, use a file sharing solution to encrypt your files and keep them safe.

AS YOUR IT PARTNER, WE KEEP YOUR BUSINESS:

PRODUCTIVE

Companies that are augmented by automation technologies are 31% more productive. We can help increase productivity.

PROFITABLE

46% of managed IT service users have cut their annual IT costs by 25 percent or more. We partner with you to increase profitability.

PROTECTED

Ransomware is 57x more destructive in 2021 than it was in 2015, with 50% attacking small businesses. Protect yourself TODAY.

Dark Web Audit

A dark web audit searches the dark web for any of your company's sensitive information.

The **dark web** is where cyber criminals go to find all manner of illegally obtained items, including private information from businesses such as social security numbers, bank account access, credit card information, medical records and more. **This is the last place you want any of your small business's information leaked.**

In order to search the dark web and find your company's leaked information, an anonymizing browser known as TOR must be utilized to hide your identity and location. We are TOR experts, which is essential for finding out if your organization is at risk on the dark web.

Claim your Complimentary Dark Web Analysis

Our complimentary dark web analysis will identify any immediate threats to your business and provide you with an exhaustive playbook for keeping your data safe. You will receive results via email in 48 hours.

CONTACT US

Meet SorceTek

Providing enterprise-level custom IT solutions and security partnerships for small businesses in Texas is our passion. Building authentic partnerships that keep your small business protected, productive and profitable is our priority.

Our enterprise-level solutions are designed for small-to-midsize businesses in any industry, but certain sectors are highly regulated or particularly vulnerable to attack. Our experience working with law firms, engineering firms, architecture firms, the financial service industry, healthcare and government agencies translates to extensive and profound expertise. We work with you to maintain compliance and exceed security standards to the highest degree in order to keep your data and your clients' data safe.

We take cybersecurity very seriously. With our focus on proactive protection and comprehensive mitigation, you never need to worry about an attack. Ransomware, malware, phishing, DDos, social engineering and security breaches are dangerous to a company's integrity, reputation and bottom line. Ascertaining security needs and potential vulnerabilities in order to provide paramount protection is critical.

SorceTek is committed to making a positive impact on all of our clients through loyalty to our customers, a pledge of excellence, taking ownership of our work, domain expertise and unmatched integrity. We are a small business and understand the importance of the organization you've built. Our Fifteen-Point Cybersecurity Checklist for Texas Small Businesses is intended to start you on the right path in protecting your organization both now and in the future.

CONTACT US

888.819.2298
info@sorcetek.com
www.sorcetek.com

6160 WARREN PKWY, SUITE 100
FRISCO, TX 75034

FOLLOW US