Keeping your business safe:

A guide to cybersecurity
Table of Contents

Activate your cybersecurity: Eight steps toward a secure business ............................................................ 3
Cyber threats impacting small businesses ............................................................................................................ 4
The potential costs of not budgeting for cybersecurity .................................................................................... 5
Creating an effective cybersecurity plan ............................................................................................................ 6-7
A look at cybercrime by industry .............................................................................................................................. 8
Cybersecurity measures for the cloud-based small business .................................................................. 9-10
Experiencing a breach: How a business owner overcame a hack ............................................................... 11
Training your employees to spot suspicious activity ...................................................................................... 12
Partnering with your bank ....................................................................................................................................... 13
Cybersecurity and beyond ....................................................................................................................................... 14
Defining cybersecurity: A glossary of terms to know .................................................................................. 15-16
Activate your cybersecurity: Eight steps toward a secure business

Read on for a deeper look at cybersecurity risks and strategies, and keep this list handy when creating or updating a strategy for protecting your business from cyber threats.

1. Understand your unique cybersecurity needs

Proactive measures should be the cornerstone of your business cybersecurity plan. Create a plan suited to your company and conduct a risk assessment and review it periodically to make sure it addresses all potential threats. When determining your cybersecurity needs, consider the types of breaches most relevant to your industry. For instance, if your business is cloud-based with numerous connected devices, you'll need a plan detailing how your employees access and treat secure information. These considerations may help you determine your specific approach to tackling cybersecurity.

2. Separate — and understand — systems and information

Keep your payroll system, business email, and point-of-sale (POS) system on separate devices to avoid a potential breach or hack impacting them all at once. Also work on basic asset management to understand what can connect to your network and who has access to what.

3. Build a backup system

Work with your third-party technology and software vendors to ensure your information is backed up regularly. Also keep a POS system that is not linked to your current network in reserve to maintain access to sales data.

4. Install and update anti-virus software

Secure your business by installing anti-virus, anti-spyware, and anti-malware programs, as well as a firewall. Check if your technology vendors offer additional protective software for mobile phones or tablets. For those devices, use a firewall with a virtual private network, which may help protect them on public networks — such as in airports, coffee shops, and convention centers. Since out-of-date software can pose a greater security risk, ensure that your software is routinely updated or patched to fix bugs, and that your hardware is on a maintenance check schedule.

5. Change default usernames and use strong passwords

When setting up a device, make sure all the default names, usernames, and passwords are unique, and don't reuse passwords across multiple sites. For example: “Admin” is easy to remember, but it's also often the standard username, and easy to guess. For increased security, use long passwords (or “passphrases”) and a combination of letters, symbols, and numbers in your passwords. Additionally, password management software can help minimize unauthorized use of a login and manage various passwords across accounts.

6. Train employees and outline specifics

Define and create roles so access is only granted as needed. Track which hardware each employee can access, and inform employees of the proper procedure when they are prompted for device updates or in the case of lost or stolen devices. Train employees to keep an eye out for issues like irregularities, bad connections, pop-ups, or phishing. And if you're considering a “bring your own device” policy (BYOD), consider the impact of employees using their own devices at work.

7. Remove employee or contractor access immediately after termination

Dedicate time to changing passwords and closing username profiles for any terminated employees. A thorough review of their computer or device will reveal any other profiles or accounts that may be accessible from that device.

8. Don’t forget about your smartphone

Have a passcode, only download applications from trusted developers, install updates regularly, and don’t click on links received in suspicious or unsolicited texts — the latest way hackers are gaining access to your data. Additionally, enable remote tracking and data wiping on your device, so if it's stolen, you can render your data irretrievable.

Keep reading for more on Wells Fargo’s perspective on the importance of cybersecurity for small businesses.
Cyber threats impacting small businesses

Peter Makohon, senior vice president of cyber threat management at Wells Fargo, explains the particular cyber threats facing small businesses.

Wells Fargo Works: What about smaller businesses makes them vulnerable to cyber threats?

Makohon: Small businesses might not have the necessary support and expertise needed to properly secure their organization’s use and dependency on internet-based services. Additionally, they aren’t always focused on operational security, and as a result, they might not fully understand their systems. This leaves them open for an attacker to find vulnerabilities.

Wells Fargo Works: What cyber threats are most applicable to small businesses?

Makohon: Many small businesses are seeing increases in ransomware attacks that threaten to encrypt and/or erase data unless a ransom is paid. In some cases, an employee that accesses a personal email account while at work or brings in a portable USB storage device can unintentionally open a file that has been infected with ransomware, banking trojans, or malicious software known as “backdoors” that can allow the attacker to remotely control the victim’s computer. Small businesses are also being targeted with wire transfer fraud that uses social engineering to trick an employee into wiring a large amount of money to an account that is under the adversary’s control.

Wells Fargo Works: What areas of a small business might these threats target?

Makohon: Threats such as ransomware typically target the contents of hard drives that are used by application servers, desktop computers, and laptop computers. In some cases recent backups are not available and the business is essentially “locked out” from being able to conduct certain electronic business. Wire transfer fraud often targets finance personnel such as controllers or accounts payable.

Wells Fargo Works: How can small business owners stay on top of the latest in cyber threats and cybersecurity?

Makohon: Businesses should ensure that IT systems are being patched and upgraded with the latest security fixes by subscribing to vulnerability and threat intelligence reports. There are a number of free and commercial sources of this information that can be set up to provide alerting based on the type of technology that the business is operating.

Read on for a look at the potential costs of not having cybersecurity protections in place.
The potential costs of not budgeting for cybersecurity

Cyber breaches can cost businesses money, customers, and their reputations, yet many admit to not having security resources in place. Take a look at the numbers behind this trend.

What can a breach cost?

A single company can spend more than $1 million recovering from damage or theft of IT assets. Disruption to normal business operations can take an even larger toll, depending on the level of damage or theft.

What business do you stand to lose?

22% of breached organizations lost customers
40% lost more than a fifth of their customer base
29% lost revenue
23% lost business opportunities

Why aren’t businesses protected from cybersecurity?

52% of respondents to a Ponemon survey say their organizations don’t have adequate budget for cybersecurity protection.
54% say their companies don’t have a password policy in place.
48% say they don’t have the in-house expertise to achieve strong cybersecurity.

Investing in cybersecurity protection isn’t a risk, but leaving your company exposed can be. Review your budget and allot what you can toward protecting your strategy documents, financials, payment information, and personnel information.

Make sure your business is protected from these risks. Read on to explore the elements to account for in a cybersecurity plan.

Creating an effective cybersecurity plan

Review these essential areas and understand how to factor them into your cybersecurity plan.

Creating a cybersecurity plan for your business is the first step you can take to help mitigate your cyber risk. While there isn’t one plan that will work for every business, there are some basic security principles that any business can follow, no matter its size.

Small business leaders are often held back by the amount of time it can take to develop a cybersecurity plan. But waiting to respond to a hack can be even more devastating. To take the first step toward protection, develop a cybersecurity plan that accounts for the following:

**Business information**
- Document all physical assets, such as computers and servers, and catalog who has access to each.
- Log digital assets, such as customer records and intellectual property, and track where information is stored.
- Once everything is documented, identify potential risks to the most important assets.

**Vendor standards**
- Verify vendors are compliant with regulatory requirements and other emerging standards, such as American National Standard Institute and National Institute of Standards and Technology, commonly cited as ANSI/NIST, and Payment Card Industry Data Security Standard (PCI DSS).
- Review vendor practices regularly to ensure continued compliance.
- Draft service-level agreements in vendor contracts that address security concerns.
Employees and access

- Establish standards for password complexity and frequency of change.
- Implement strong authentication measures. If it’s feasible for your business, consider two-factor authentication and single sign-on (which unifies login information with the various third-party software portals your company may use) to lessen the odds and impact of a compromised account. To explore these features, you can either download a free authentication generator or purchase a package.
- Devise a tiered/limited system for assigning administrative rights to users.
- Train employees and contractors to recognize, avoid, and report suspicious activity.

System tools

- Define and implement core protections such as anti-virus, firewall, and anti-malware tools.
- Implement software to monitor network traffic and identify suspicious behaviors — both free tools and more multifaceted purchasable packages are available, depending on your business needs.
- Explore whether your business may be able to protect and isolate sensitive data within your network using multi-layered encryption. Approaches to encryption vary in complexity from business to business, so consider which elements may make most sense for your business to encrypt.
- Decide when and how the system will receive software updates and patches.
- Pursue third-party security certifications and standards for your services and products.
- Back up local data to the cloud, and other local storage, to preserve access in case of an attack.
- Use proper settings for encryption on Wi-Fi routers.
- Provide separate networks for guest access.

Operations

- **Leadership**: Determine who is responsible for reviewing and updating the cybersecurity plan, and how often.
- **Implementation**: Determine who is responsible for training users, enforcing standards, and managing/monitoring installed software.
- **Response**: Determine who would be responsible for responding to an attack, and how. This procedure should include provisions for straightforward incidents as well as those that require an escalated response. It should also include a provision for declaring that an incident needs to be resolved.

Physical and digital protection

- **Digital**: Make it a habit to encrypt data, and install and maintain anti-malware programs.
- **Physical**: Keep computers and servers with sensitive information in a secure office location.

Leverage all this information for the creation of a digital and hardcopy cybersecurity plan you can reference as needed.

You may consider using a tool like the Federal Communications Commission’s Small Biz Cyber Planner 2.0 to make sense of these elements and develop a cybersecurity plan.

Once you have a plan in place, it’s important that you update it regularly.

It’s even more important to put it to use by training your employees according to it.

Want more insights on cyberattacks in the real world? Next up, check out the infographic on impact by industry.
A look at cybercrime by industry

Are some industries more likely to experience cybercrime? This data reinforces the importance of a comprehensive cybersecurity strategy for small businesses across industries.

Just as numerous other aspects of running a business vary according to industry, so do cybersecurity needs. Learn which industries have been identified as most vulnerable to both incidents and breaches, according to the 2019 Verizon Data Breach Investigations Report.

From the report: Total number of top three incident types by industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Incident Types</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail</td>
<td>Server</td>
<td>184</td>
</tr>
<tr>
<td></td>
<td>Hacking</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>Web app</td>
<td>92</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Server</td>
<td>259</td>
</tr>
<tr>
<td></td>
<td>Hacking</td>
<td>233</td>
</tr>
<tr>
<td></td>
<td>Denial of service</td>
<td>163</td>
</tr>
<tr>
<td>Healthcare</td>
<td>Server</td>
<td>225</td>
</tr>
<tr>
<td></td>
<td>Misuse/Privilege misuse</td>
<td>110</td>
</tr>
<tr>
<td></td>
<td>Miscellaneous errors</td>
<td>104</td>
</tr>
<tr>
<td>Accommodation and food services</td>
<td>Server</td>
<td>68</td>
</tr>
<tr>
<td></td>
<td>Malware</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>Point of sale</td>
<td>40</td>
</tr>
</tbody>
</table>

Cybersecurity planning can be tough for small businesses that store data in the cloud. Yet, it’s possible for all companies to develop and execute a plan to secure cloud-based assets, including customer data. Here are key points to consider when crafting a winning strategy:

**Seek endpoint protection**

Most security compromises start by infecting an "endpoint," or a communications-connected workstation (anything from a mobile phone to a wireless-connected printer).

Protecting the endpoint, both manually and with Software as a Service (SaaS) provider solutions, secures your computer network from remotely connected devices.

Most available solutions should include anti-virus/anti-malware (AV/AM), but also look for options that support a range of operating systems (Linux, Windows, iOS, etc.) and mobile devices (iOS, Android, etc.).

**Look for this from your SaaS**

- Ensure the service has the right certifications.
- Ensure they conform to relevant industry standards such as SOC 2, Type II certification for data security, or the PCI Data Security Standard for mobile payments.
- Check back periodically with vendors who pass your initial screening to make sure they maintain their certifications, are in compliance with emerging standards, and are regularly updating and patching their security software.
• Confirm they can help protect customer sensitive data.

• Ensure that all your SaaS products can protect sensitive information, especially if you are storing credit card or personal information.

• Explore business-focused cloud access security broker (CASB) solutions that can also integrate with data loss prevention (DLP) solutions or offer DLP add-ons. According to Gartner, CASBs are security policy enforcement points (both on-site and cloud-based), placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies.

Address encryption

Cloud SaaS data encryption

• Aim to use a CASB solution that offers encryption across SaaS providers. Though it may seem easier for a business with limited technical capabilities to turn over key management to each individual SaaS provider, it tends to be more efficient and effective to employ a single CASB encryption across services.

Wi-Fi

• Keep your business Wi-Fi’s protection settings up-to-date, and encrypt the router or firewall. Additionally, ensure internal devices and guest users connect via separate networks.

Full-disk encryption on servers and workstations

• Your operating system will likely provide encryption tools, and you can also make use of disk encryption tools from your endpoint protection solutions to manage servers and devices.

Access management

• Businesses should grant access to cloud SaaS applications as needed, which means ensuring that access is revoked when an employee leaves the company. The access control can be done via a cloud-based service like a CASB, Web proxy services, and IAM services, or a combination.

Back up everything — frequently

• Focus on backups for data from on-premise servers and workstations. Consider using cloud-based backup solutions that perform backups of both servers and cloud-based workstations. Mobile devices should also be backed up in an automated manner using cloud-based backup solutions. Consider a trial run of any new solutions so you can fully assess if a product will suit your needs.

• Not only will this protect you from hacks that encrypt data until a ransom is paid, like the notorious WannaCry ransomware attack in May 2017, but it will also serve as a failsafe against network outages or failures.

Cloud-based small businesses can't afford to ignore cybersecurity. Fortunately, by developing and executing a sound strategy, they can secure their data without losing sight of their core operations.

Next, take a look at how one such business owner experienced — and overcame — a cyberattack.
Experiencing a breach: How a business owner overcame a hack

One business owner recalls how a cyberattack affected his website, and how the business recovered.

We came into the office one day, and the phones were ringing like crazy. We’ve always told our customers to call us if they received an odd message related to their accounts with us. But in this case, the strange things they were getting were coming from us. Our server was emailing our customers weird messages, a lot of it in foreign languages. At the same time, we were receiving thousands of web form submissions in different languages and hits on our website from all over the world — Russia, Spain, and France. This was strange, because we’re a U.S.-based company and can only work with U.S. citizens.

The attack had completely overwhelmed the site. The attackers were using a process of bots, hitting the site over and over. They got inside our actual files and placed code on the individual pages that was routing the information to a new server.

Halting business

On that first day, we pulled down our entire website. The web developers I work with told me they could remove just the malicious code, but I said, “I don’t care. I want it all gone.” Since we are mostly online-based, it shut our whole business down. We pulled every file down from our server and started from scratch.

Our accounts hold information like customers’ names, addresses, and dates of birth — things that would be valuable to the dark web community. In this situation, we were especially fortunate that our payment processing runs through a third party. We are fully PCI-compliant and don’t store credit card numbers. Even on accounts dealing with customers’ finances, we don’t store the full account number ourselves.

Communicating the breach

Immediately, we sent a mass notice to every one of our customers. We explained what could have occurred and what personal information could possibly have been compromised. We also encouraged customers to contact us if they had any issues or needed help with their file.

The business takes in about $100,000 to $150,000 a month in revenue, and we lost 10 to 12 days while the website was being rebuilt. We also rely heavily on referrals, so we definitely lost additional customers beyond the signups we missed during that downtime. And we had another $10,000 to $12,000 in site costs. Altogether, this cost us about $50,000.

Taking action

Ultimately, we decided to move to a different web-hosting company. We also added some code to the website that monitors changes. If the site gets changed and we weren’t the ones that did those changes, we’d know it as soon as it occurred. We haven’t had a notice since. We also took the opportunity of rebuilding the website to relaunch with a new logo and an improved look and feel.

We have always taken privacy very seriously and continue to take every available measure to protect our customers’ information.

Keep reading for more on the important role of employees and contractors in maintaining your cybersecurity.
Training your employees to spot suspicious activity

By knowing what to look for, your employees may lessen the impact of a breach — or stop one in its tracks.

Teaching employees how to recognize suspicious activity may help save the resources it takes to recover from an attack.

Examples of suspicious activity your employees should look out for:

1. **File irregularities:** Malicious attackers will often alter critical system files, so identify files that have moved, deleted, or changed without explanation.

2. **Sluggish connections:** If systems suddenly begin to crash or slow down, notify your IT department or an identified company contact. When a device or network’s performance inexplicably drops, the culprit is often a virus or malware.

3. **Excessive pop-ups:** Sudden upticks in pop-up messages, fake virus alerts, or redirect messages that divert the user to another site could be signs of an attack.

4. **Strange emails:** Emails with strange links or senders can be cyber attacks. Delete the email immediately without responding or clicking any links.

Make sure employees exercise caution. Computers can occasionally hiccup, but anything out of the ordinary should be investigated.

Hold periodic meetings to review data security. Familiarize new hires with your security protocol to ensure everyone involved learns to spot possible attacks.

---

### Keep your business safe

The more people gain access to your information, the more your business is open to security risks. Learn what you can do to protect your business while working with contractors.

**Build a foundation for your security policy**

- Implement a security policy among employees and contractors.
- Use a contract that emphasizes the importance of protecting critical data, and holds all employees accountable for preserving it.
- Make sure you receive signed agreements from everyone you employ.

**Assign varying levels of information access**

- Determine how much access each person actually needs.
- Contractors may work for you short-term then move to another company. Set processes to revoke access after they leave.

**Make it an ongoing conversation**

- Send out regular reminders on threats and keeping data safe.
- Have employees who monitor your data. In the event of an attack, you’ll be able to see what information was affected.

---

To learn more about steps you can take to help protect your business, check out our full guide on cybersecurity.
Partnering with your bank

Your financial institution may help give you some peace of mind when it adheres to thorough cybersecurity measures. Learn more about what to expect.

Most financial institutions continue to concentrate on investing in and leveraging a wide range of advanced technologies to bolster security. However, small businesses should do the necessary research to make sure the protection offered aligns with their business objectives.

For instance, here are a few examples of best practices from a financial institution:

1. The organization uses multifactor authentication.
2. Strong encryption software is in place to help protect accounts and critical data, and the institution only supports browsers that adhere to high encryption standards.
3. They continually monitor for suspicious activity, including restricting account access to prevent certain types of transactions.
4. They employ advanced security controls for payment transactions, with vulnerability and patch management programs continually kept up-to-date.
5. Employees and third-party suppliers are required to follow formal information security policies.
6. Comprehensive cyber incident and business continuity plans are in place for potential cybersecurity risks.

Because cyber threats are ever changing, organizations such as Wells Fargo continue to prioritize the advancement of these types of security measures to help protect financial information, monitor the threat landscape, and adapt security measures to address emerging threats. Wells Fargo is proactively advancing its security to help protect your financial information with evolving technology and committed support.

Learn what Wells Fargo is doing to protect your financial information.
Cybersecurity and beyond

You’re now in a better position to assess your business’s cybersecurity needs, and determine the best way forward for your business. To get started, ask yourself: Do I know where all my data is stored? Who has access to all my files and documents? How do I encrypt data? Continue to have discussions with your team and technology advisors, and leverage the information in this guide as well as additional reliable sources to build an effective and proactive cybersecurity strategy:

- The Department of Homeland Security
- The Small Business Administration
- StaySafeOnline by the National Cyber Security Alliance
- United States Computer Emergency Readiness Team
- Better Business Bureau: BBB Scam Tracker


Discover more cybersecurity tips and the additional resources and education that Wells Fargo Works for Small Business® offers. Visit [wellsfargo.com](http://wellsfargo.com) to access an array of content for every aspect of your business: financials, business planning, marketing, management, and insights from other business owners. And, revisit this guide as an active part of running your business and moving it forward.
Defining cybersecurity: A glossary of terms to know

Ensure you and your team are familiar with cyberattack terms and definitions ahead of encountering suspicious activity in your day-to-day business.

**Black hat hacker:** This cyber criminal uses technical skills to find or develop software holes and attack methods to hack into machines and steal data, such as passwords, emails, intellectual property, credit card numbers, or bank account credentials.

**Breach:** An incident in which data is intentionally (or unintentionally) released from a secure environment by an unauthorized source, such as a black hat. There must be confirmed disclosure of sensitive information, such as banking details or intellectual property, targeted by the hacker for the incident to qualify as a breach.

**Cyber-espionage:** Also known as cyber spying, this is the theft of intellectual property or classified material stored online, for which hackers may use a variety of methods. The confidential information can be obtained without the knowledge of the holder via computer networks, servers, or malicious software.

**DDoS, or “distributed denial-of-service”:** This is a cyberattack that uses several hacked computer systems to attack one target and take it offline. Hackers will use malware to gain access to a host of machines that will then flood a website’s server with a high volume of traffic. This makes it impossible for people to load the page, thus effectively taking it offline and leaving the site’s services unrenderable.

**Hacking:** A majority of security breaches (52%) are conducted by way of hacking, which is the unauthorized intrusion into a data system using a computer. Stolen credentials played a role in 29% of breaches.

**Incident:** An event compromising the integrity of secure information. Unlike a breach, information is not confirmed as disclosed to an unauthorized party when classified as an incident.

**Lost and stolen asset:** An incident that compromises the integrity of information when a device containing sensitive data goes missing, whether through genuine loss or theft. However, encrypting individual devices can diminish the impact of a lost or stolen asset.

**Malware:** Also known as malicious software, this is an umbrella term for any software that adversely affects your computer operations. Common synonyms are virus, trojan, and worm. Approximately 51% of breaches include malware, but can be mitigated using security suite software like Windows Defender and Symantec.

**Payment card skimmer:** A device that criminals place on an asset that reads credit cards, such as ATMs or POS machines, at unsuspecting, legitimate businesses. Skimmers access sensitive information from the transaction for use at a later time.
Privilege misuse: Privilege misuse is when someone accesses accounts containing administrative data or uses data that holds monetary value for destructive or criminal purposes. This type of breach is generally internal, but can involve external parties when collusion is involved.

Ransomware: This is another form of malware that encrypts files and prevents users from accessing their systems until they pay a ransom.

Social engineering or phishing: This occurs when cyber criminals try to trick you into giving them information by creating profiles, fake emails, and other schemes in which they pose as someone you know — a family member, friend, or coworker, for example — and asking for personal details.

Spyware: A subcategory of malware specifically designed to gather data about you and transmit it to an attacker. Spyware programs called keyloggers can record every keystroke you put into your keyboard and send that information to the attacker.

Web app attack: An incident in which a web application is infiltrated to steal data or perform unauthorized transactions.

White hat: The counterpart to black hat hackers, white hats are security professionals hired by businesses to intentionally hack into the organization’s systems to expose vulnerabilities.


Strategies and tips provided in the guide are general in nature for your consideration and are not legal, tax, or investment advice. Wells Fargo makes no warranties as to accuracy or completeness of information, does not endorse any non-Wells Fargo companies, products, or services described here, and takes no liability for your use of this information. Information and suggestions regarding business risk management and safeguards do not necessarily represent Wells Fargo’s business practices or experience. Please contact your own legal, tax, or financial advisors regarding your specific business needs before taking any action based upon this information.

© 2020 Wells Fargo Bank, N.A. All rights reserved.