ACKNOWLEDGEMENTS

The Guide to Cybersecurity for Small and Medium Businesses was developed with guidance from the U.S. Agency for International Development (USAID) Bureau for Development, Democracy, and Innovation’s (DDI) Center for Economics and Market Development (EMD) and principally authored by Daniel Vazquez under the Trade and Competitiveness Activity implemented by Resonance Global. Additional contributions and review were provided by Clare Sullivan of the Cyber SMART Research Center at Georgetown University, as well as Jeremy Ravenelle, Evan Legé, and Anne Szender McCarthy of the Trade and Competitiveness Activity.

This document was produced for review by the United States Agency for International Development. It was prepared by the Trade and Competitiveness Activity, contract number AID-OAA-C-17-00110. Its contents are the sole responsibility of the author and do not necessarily reflect the views of USAID or the U.S. Government.
TABLE OF CONTENTS

Glossary of Terms .................................................. 2
Acronyms List ..................................................... 3
Introduction ......................................................... 5
   The Importance of a Good Leader ......................... 5
Where to Start ...................................................... 7
   1. Train employees to trust but verify .................... 7
   2. Install reputable antivirus and antimalware software 8
   3. Use network firewalls .................................... 8
   4. Set strong passwords .................................... 8
   5. Use multi-factor authentication ....................... 9
   6. Regularly update software ............................. 9
   7. Encrypt all sensitive data .............................. 10
   8. Secure Wi-Fi connections .............................. 10
   9. Monitor payment systems ............................. 11
  10. Keep the business website secure .................... 12
  11. Prevent mobile phones from being targets .......... 13
  12. Keep backups of all information .................... 14
  13. Remember that physical security is part of cybersecurity 15
  14. Explore the possibility of cyber insurance .......... 16
  15. Consider hiring an IT professional .................. 17
If a Cybersecurity Incident Occurs ......................... 18
   Restoring Operations ....................................... 18
   Managing Communications Effectively ................. 19
      Notify the Authorities ................................ 19
      Notify Service Providers ......................... 20
      Notify Clients and Customers .................... 20
   Social Media ................................................... 21
   Learning from the Incident ............................ 21
Conclusion ......................................................... 22
GLOSSARY OF TERMS

Antivirus software: A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents, sometimes by removing or neutralizing the malicious code.

Cryptocurrency: A digital currency in which transactions are verified and records maintained by a decentralized system using cryptography rather than by a centralized authority. Examples include Bitcoin, Ethereum, Monero, etc.

Cyber attack: An attack via cyberspace that targets an organization’s use of cyberspace, for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure or to destroy the integrity of the data or to steal controlled information.

Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Distributed denial-of-service (DDoS): A form of cyber attack in which the attacker renders the target machine, website, or network unavailable to its users by flooding the target with requests in an attempt to overload the system.

Encryption: The process of transforming plaintext into ciphertext.

Firewall: A capability that limits network traffic between networks and/or information systems.

Firmware: Computer programs and associated data that may be dynamically written or modified during execution.

HTTPS: A combination of the Hypertext Transfer Protocol (HTTP) with the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol. TLS is an authentication and security protocol widely implemented in browsers and web servers.

Malware: Software that compromises the operation of a system by performing an unauthorized function or process.

Modem: A device that converts digital data to be transmitted over a network—for example, a device that allows a home or business network to interface with an Internet service provider (ISP).

Multi-factor authentication: Authentication using two or more different factors to achieve authentication. Factors include: something you know (e.g., password or PIN); something you have (e.g., cryptographic identification device or token); or something you are (e.g., biometrics).

Router: On a network, a device that determines the best path for forwarding a data packet toward its destination—for example, a device that emits a Wi-Fi signal.

Secure Sockets Layer (SSL): Provides privacy and data integrity between two communicating applications. It is designed to encapsulate other protocols, such as HTTP.

Service Set Identifier (SSID): The name of a Wi-Fi network.

**ACRONYMS LIST**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS</td>
<td>Distributed Denial-of-Service</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>NIST CSF</td>
<td>National Institute of Standards and Technology Cybersecurity Framework</td>
</tr>
<tr>
<td>PCI</td>
<td>Payment Card Industry</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
<tr>
<td>WPS</td>
<td>Wi-Fi Protected Setup</td>
</tr>
</tbody>
</table>

1. [https://niccs.cisa.gov/about-niccs/cybersecurity-glossary](https://niccs.cisa.gov/about-niccs/cybersecurity-glossary)
2. [https://www.oed.com/](https://www.oed.com/)
5. [https://csrc.nist.gov/glossary](https://csrc.nist.gov/glossary)
12. [https://www.oed.com/](https://www.oed.com/)
INTRODUCTION

This second section of the Guide to Cybersecurity for Small and Medium Businesses introduces a range of practical strategies that small business owners can implement to protect their organizations from cybersecurity threats. This starting point can help owners to become more comfortable with the ideas and strategies that this guide explores. For greater depth, small business owners should consult more advanced resources on the Internet or seek the advice of an IT professional.

From a business’s point of view, it might seem logical to approach cybersecurity solely from a legal compliance perspective. Although this can be a first step in the right direction, businesses should assume that innovation and new technologies rapidly outpace regulations. There are relatively simple actions that businesses can take to drastically reduce the likelihood and impact of cyber attacks. At the same time, despite the best preventive practices, it is likely that at least one attack will succeed, making it necessary to create resilience within the business and to establish the ability to bounce back after a breach.

The Importance of a Good Leader

Organizations of all sizes confront the question of who should lead cybersecurity. The Harvard Business Review article on rethinking cybersecurity leadership argues that the person who leads and is responsible for cybersecurity in the organization should be “an influential voice in business strategy, technology decisions, and enterprise risk management,” rather than someone who only has the technical expertise. Businesses need to embed cybersecurity awareness and good practice across the organization, covering all elements—technical, business planning strategy, and people, including customers, suppliers, and employees.

13 https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is
WHERE TO START

Many businesses are likely already implementing some cybersecurity steps as part of an IT security posture that if supplemented, can greatly reduce risk. These actions, known as “cyber hygiene practices,” are relatively simple, routinely done, and can have a positive impact on businesses’ digital security. Cyber hygiene best practices include:

1. Train employees to trust but verify;
2. Install reputable antivirus and antimalware software, and keep it up to date;
3. Use network firewalls, and check them routinely;
4. Set strong passwords, and change them frequently;
5. Use multi-factor authentication;
6. Regularly update software;
7. Encrypt all sensitive data;
8. Secure Wi-Fi connections;
9. Monitor payment systems;
10. Keep the business website secure;
11. Prevent mobile phones from being targets;
12. Keep backups of all information;
13. Remember that physical security is part of cybersecurity;
14. Explore the possibility of cyber insurance; and
15. Consider hiring an IT professional.

1. Train employees to trust but verify

As a rule, employees should only have access to the resources and information necessary to perform their job functions. To determine this, a business needs to know how data, systems, devices, etc. are used and for what purpose. Whenever possible, businesses should create user profiles—i.e., accounts that limit access to specific resources within the business. When this is not possible, the next best action is to set restrictions and to password protect access to folders or files as a part of the functionality of operating systems. Key to limiting access is also terminating access once an employee leaves the company. This will mitigate the risk from insider threats. If a business wants robust controls, there are many IT solutions that can facilitate the creation and management of user profiles. Administrators can talk to an IT professional and should consider contacting the Help Desk for their operating system to learn which methods of controlling file access are appropriate.
MITIGATING RISK: USER ACCOUNTS

After understanding what the business’s information is and how it can put the organization at risk, businesses should identify who has access to which data. They should:

- **Put together a complete list of user accounts** used for accessing all the services, devices, applications, email addresses, cloud services, databases, phones, tablets, Internet of Things (IoT) devices, business systems, etc. They need to know and record who uses them, including outside vendors who have access.

- **Identify each user and the data streams to which they have access, and mandate the use of different passwords for each function or system**, especially for those containing restricted information.

- **Direct users to not share accounts and to password protect critical data.**

2. Install reputable antivirus and antimalware software

The most common solution to protect against malware is antivirus software. Microsoft Windows, Google Chrome, and Mac operating systems already have built-in antivirus software that performs well against most threats and that have the basic functionality to detect and remove malware, when kept up to date. Despite the advantages of these built-in programs, attackers have ample opportunity to design malware programs to circumvent these defenses. It is a good practice to include additional antivirus protection on business IT devices and to ensure it is regularly updated.

3. Use network firewalls

“Firewalls” are devices or programs that control the flow of information or traffic between networks (network traffic) from an external network to the business, within the business’s internal network, or between devices with different security configurations. Firewalls can be integrated in the router provided by the Internet Service Provider (ISP) or in specific antivirus programs. A firewall is an essential defense for a business. Depending on the level of business risk, businesses should consider whether to upgrade firewalls and complement them with other solutions, such as those that encrypt traffic or closely monitor information exchanged with and within the business network.

4. Set strong passwords

Simple, one-word passwords used in the past are no longer an effective means to protect an account. Attackers now have tools capable of cracking passwords within an hour or less. A more secure practice is to develop passwords with short phrases.
containing mixed numbers and special characters to make passwords complex, longer, and harder to guess. Examples of such phrased passwords are #Sl33pWe11, Sc0r3G0a1!, and K0mbuchaP0w3r*.

MITIGATING RISK: PASSWORD PROTECTION

Passwords should always be complex, kept in a safe place, kept confidential, and regularly changed. One of the most common vulnerabilities for businesses is employees writing down their password on a note attached to their computer or placed somewhere else near their work area, threatening data security. Digital “wallets” can securely encrypt stored passwords.

Businesses should have one password for each system or website and should ensure that they are changed regularly or at least once a year. If a site allows longer passwords (20 or more characters), users can create full password sentences, like “I'd like a long vacation!”

Systems’ administrative interfaces generally allow customization of password requirements, including the frequency for changing them. Businesses should use those functionalities to create password specifications that work for the desired security of the organization.

5. Use multi-factor authentication

The use of multi-factor authentication has become popular during the past few years. “Multi-factor authentication” requires users to provide two or more means of verification to gain access to an account, application, or system. It can be a combination of a password or other information specific to the legitimate user and a code that is generated and sent by the system (via email, text message, or phone call) to the user. Many technology platforms, including single sign-on providers, payment systems, and various user accounts, now use multi-factor authentication. If it is available, businesses should make sure that it is enabled for both internal (employee) and external (customer) accounts, as applicable.

6. Regularly update software

With updates, developers fix or “patch” problems, including known security vulnerabilities to apps, programs, or operating systems. These updates should be installed as soon as possible. Businesses should keep in mind that developers only can fix known vulnerabilities. If a problem goes undetected, a business will be vulnerable, even if all of its IT systems

14 https://www.av-test.org/en/antivirus/home-windows/
15 Well-known publications, like PC Magazine, frequently run tests on free antivirus software and firewalls, reporting their findings to the public. Examples of the reviews can be found here: https://www.pcmag.com/picks/the-best-free-antivirus-protection
16 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf
are consistently updated. This is a risk to be prepared for, but regularly updating the business software will mitigate much of that risk.

7. Encrypt all sensitive data

Encrypting data makes the contents readable only to those who have the keys or passwords to open or decrypt the data. Individual files or whole devices, including cloud drives, can be encrypted. There are many encryption solutions available, with both Microsoft and Apple offering built-in encryption tools, such as BitLocker and FileVault, respectively. The downside of these tools is that if the key or password is lost, the data cannot be recovered. Be sure to make a copy of the key in a secure place or have a way of securely remembering the associated password.

8. Secure Wi-Fi connections

Wi-Fi devices are usually provided by ISPs as boxes that have a “modem” (the equipment that connects the business to the provider’s network) and a “router” (the equipment that broadcasts the Wi-Fi signal within the place of business) combined into one. Typically, a technician installs this box upon initial Internet installation and the box remains untouched until the ISP changes it out or the equipment fails and needs to be replaced. ISPs buy large quantities of these devices, and their security considerations for consumers do not necessarily align with an individual business’s security requirements. The devices will likely need to be tailored to meet a business’s cybersecurity demands. To increase the protection that a router can provide, there are some actions that can be done with little or no cost:

a. **Change the password to access the ISP router settings.** The router has an interface that lets administrators make changes to the device’s configuration. Routers come with either a generic or an ISP-assigned password to access their settings. Following the instructions in the device’s manual, administrators can change the generic password to a new, strong password. Admins should keep that new password in a safe place and only share it with the appropriate people.

b. **Update the business’s ISP router’s firmware regularly.** “Firmware” is the router’s operating system. With the knowledge to access the router settings, administrators follow the manufacturer’s instructions to check for and install updates. In accordance with the business cybersecurity plan, they regularly check for new updates and install them as needed. They need to locate the device’s end-of-support date and plan ahead to replace it at that time.

c. **Always enable security, i.e., encryption protocol.** To connect to Wi-Fi, and frequently change the password to access it. If the router supports a guest network, administrators should enable it and use it for anyone or anything that does not need access to the business’s IT systems, including guests, outside vendors, and private IoT devices. Wi-Fi encryption protocols secure the connection between the router and the device that is connecting to it, such as a laptop, but not the communications over the Internet. This makes it necessary to also frequently change the guest network.
password. Wi-Fi encryption is continuously evolving with Wi-Fi Protected Access (WPA) and its more secure replacement, WPA2, now commonly supported by devices. Businesses need to enable the most advanced protocol possible and to replace the default Wi-Fi password (also called a “passphrase”) with a strong and unique password, even if the default one seems difficult to crack. WPA2 accepts a range of 8–63 characters, which should be sufficient to accommodate network passwords, such as MaryHadaLittleLamb, LittleLamb, LittleLamb, MaryHadaLittleLamb. The reality is that business Wi-Fi passwords are often shared with outsiders, so it is a good practice to regularly change them as part of the business cybersecurity plan and to ensure that the internal, non-guest password is secure and not posted publicly.

d. Disable easy Wi-Fi connection. An example is the single-button Wi-Fi Protected Setup (WPS) technology. If the router is not physically secured, anyone that has physical access to the router can use this function to penetrate its network.

e. Change the Wi-Fi name. The Service Set Identifier (SSID) is the Wi-Fi name. Change the default SSID to one that does not reveal personal information and does not provide information about the device being used, such as the router’s make and model or the ISP, so as not to facilitate an attack.

f. Research the implications before making other changes to the router. Enabling or disabling a functionality can open or close doors to attacks or limit the functionality of the device.

g. Test. After the changes are implemented, run tests to see whether they are working as intended.

h. Add your own router. It is not unusual that small business environments are provided consumer-grade routers, with ISPs reserving more sophisticated equipment for larger clients. A small business can improve its Wi-Fi security and its control over the router’s functionality by adding its own router connected to the ISP-provided router/modem. Admins can contact the ISP to discuss how to implement this setup, or search manufacturers for options.

9. Monitor payment systems

Depending on the model of the small business, payments will be received in different ways, e.g., via point of sale, the business’s website, an app, or a third-party merchant site, and each one presents specific challenges to cybersecurity. The Payment Card Industry (PCI) Security Standards Council, an organization that develops security standards related to payment methods, has created comprehensive guides\(^\text{9}\) about the potential risks of these different systems, including Internet-connected payment terminals or payment apps. The guides also advise on actions that can be taken to mitigate risk. Many of the mitigation actions relate to cyber hygiene practices (e.g., updating software and using strong passwords) because payment systems are also connected devices.

---


Encryption of consumer payment card data during transit to the payment processor and within the merchant systems is particularly important.

10. Keep the business website secure

A website is a tool to interact with consumers, provide services, or sell products, and it largely establishes a business’s digital identity. The best way to secure this critical asset depends on the site’s technical properties, the IT ecosystem in which it is managed, and where the site is saved or hosted. Many businesses use cloud services that offer easy-to-use website builder tools. These solutions ease the burden of creating and managing the site and transfer some responsibility for protecting and monitoring the IT infrastructure to the host provider. However, websites can still be at risk if they are improperly coded by the building tool, plug-ins, extensions, or third-party services that are incorrectly configured or have vulnerabilities.

**MITIGATING RISK: WEBSITE SECURITY**

Match the level of resource allocation needed to secure the business website with the level of the website’s importance to the business and the inherent risks inherent. It is good practice to:

1. **Have robust requirements for administrator login credentials.** Limit the number of people who have administrator privileges.

2. **Use a reputable website host and builder software to develop and maintain the site.** Reputable companies are likely to have good security suites, like firewalls, antimalware, monitoring, and distributed denial-of-service (DDoS) prevention options, to protect hosted sites and scalable features.

3. **Regularly update site software.** This includes the platform, the website’s software, and any additional programs coded in the site, e.g., plug-ins, extensions, and third-party integrations.

4. **Use HTTPS protocols.** This requires installing Secure Sockets Layer (SSL) certificates that encrypt information between the website and the user.

5. **Require strong passwords if the website allows users to create accounts, and enable functionalities to lock down accounts after multiple unsuccessful login attempts.**

6. **Create a “cyber pen” around files that users upload.** This requires having measures in place to ensure that files are safe, including antivirus and antimalware scanners of an allowable type. It is advisable to limit the type and size of files that are accepted for upload and to have a program that checks the file type and ensures that the file is uploaded to a safe location outside the folder where sensitive information is stored or where there is access to all website files.
7. Regularly back up the site, including all of its data. The frequency of backups depends on how critical the data are, but ideally backups should be done daily. If possible, business should have an automatic service for backups. In cases where the website and its data are critical to the business, organizations should consider doing redundant backups and keeping backup data in different locations to have access to the data in case of a natural or political disaster or cyber attack.

II. Prevent mobile phones from being targets

The number of smartphone users is steadily increasing, with over 3.4 billion currently estimated worldwide. Many smartphone users bring devices to the workplace or use those provided by employers. What sets mobile devices apart from work computers is the amount of personal and work data that the devices can save and that they are always online. Additionally, their portability puts them at a higher risk of being lost or stolen. A hacker who can access a phone, either physically or by infecting it with malware, can penetrate a business’s network. Keep in mind that a business has more control over mobile devices that it furnishes to its employees than it does over personal devices brought by those employees into the business environment.

MITIGATING RISK:
SECURING MOBILE DEVICES

Businesses can improve the security of mobile devices by following general cyber hygiene practices (e.g., update apps and operating systems, install reputable programs, configure to use secure connections, use trustworthy Wi-Fi networks, etc.). In addition, there are some precautions that apply only to smartphones. Businesses should:

1. **Purchase devices that can be remotely wiped of data and that use strong security features.** A common method of wiping a phone is to use a web-based interface managed by the manufacturer of the device or the operating system developer. Both Apple and Android have this functionality. Strong security allows a user to encrypt all the information stored on the phone with backup to the cloud or a personal computer, and a strong password or biometric information is required to unlock the phone. Business should use all of these methods.

2. **Use and update the manufacturer’s operating system.** Often users replace the original operating system with one created by a community of developers. This process is called “rooting” or “jailbreaking.” Since the security of a rooted and

---

20 Companies like Wix, Squarespace, or Weebly have been recognized globally for their products and services. There might be other domestic or regional companies that could provide comparable products.
21 Distributed denial-of-service (DDoS) is a form of cyberattack that overwhelms a target server with requests eventually resulting in that target rejecting legitimate service requests. This ends up disabling the website.
23 https://support.apple.com/guide/icloud/erase-a-device-mmfc0ef360/icloud
24 https://support.google.com/accounts/answer/6160491?hl=en
jailbroken operating system is difficult to ensure, those devices should not be granted access to the business’s network or sensitive data.

3. **Avoid clicking on suspicious links, especially in text or messenger apps.** As explained in the previous section, links in messages can be used to deliver malware and launch an attack.

4. **Be vigilant about apps and restrict the data that apps can access.** Researchers are routinely analyzing apps for security concerns, such as in the well-known recent debate involving TikTok and WeChat. Avoiding apps from outside the operating system’s official stores (e.g., Google Play and Apple App Store) and restricting the data that apps can access after installation are good cybersecurity practices. Businesses should try to limit apps’ access to other resources, such as location, contacts, file folders, information from other apps, and camera.

5. **Disable functions when not using them.** Smartphones have many ways to connect, in addition to cellular networks, including Bluetooth, Wi-Fi, and AirDrop. Each of these are potential avenues for an attack. Admins should only turn on the necessary functionalities when needed.

6. **Delete.** After a cell phone has been disconnected from a business’s network, all business-related data should be deleted from it. If possible, the cell phone should be completely wiped clean of all data.

---

**COSTS OF DISRUPTION**

In 2014, global research firm Gartner found that the average cost of business downtime was $5,600 per minute. For a business, this cost might be less, depending on the organization’s characteristics, country, and sector, but it is reasonable to estimate that without a cybersecurity plan the costs of bringing the business back online will amount to several days of operational costs, even in the best-case scenario.

**12. Keep backups of all information**

Nowadays, most businesses are heavily reliant on data and information technology (IT) systems. When planning for cybersecurity and creating backups, organizations should understand how the systems work and should prioritize backups for the most sensitive information and critical systems. As the business matures, administrators should start thinking about getting more sophisticated systems that help recover operations more quickly after an incident.

With the arrival of free and affordable cloud storage, some businesses believe that these systems provide adequate backup. Although most do provide backup, if cloud storage is synced with a computer, an attack to the original system, file, or the cloud service can extend to the additional stored data, so that type of protection alone might not be sufficient. Businesses should take full advantage of reputable free cloud solutions as an initial step for safeguarding data. They should also keep in mind the limitations, which include their inadequacy for making backups of certain types and sizes of files, incompatibility with file names, and the potential to lose data from the time it was last saved to the time of the next backup. A good example is a small business that produces videos. Those files are very large, difficult, and comparatively slow to back up to cloud services. Losing days or weeks of unsaved data can be very costly. In some countries, the free solutions might not be adequate to comply with regulations.
A good backup strategy should save programs and operating systems—not just data. In other words, it should aim to create a comprehensive copy or image of all the information on the hard drives used by the business’s computers. In the event of an incident, that image can be loaded back onto a clean or new computer, reducing the recovery time. Using specialized software, backups can be saved locally (on the computer’s own storage), to external drives or media, to a cloud service, or in a hybrid scenario using both local and cloud storage.

**MITIGATING RISK: BACKING UP DATA**

**Businesses should back up their data often and, if possible, automatically.** If the organization does not have an automatic solution, it needs to budget the time to manually create full backups. That is a factor when considering the level of tolerance to data loss applicable to a business. Microsoft and Apple operating systems, as well as many mobile operating systems, offer backup functionality that can be used as a starting point.

Backups can get corrupted or lost, or the media used to save them can become outdated, so it is wise to make multiple copies using different media. One copy should be kept off-site to protect it from a catastrophic incident, like a fire or building collapse, and all copies should be encrypted.

Some businesses may have the additional challenge of a lack of interconnection or standardization of its systems. Employees may not all have the same computer or operating system, and business information could be spread across computers and devices tailored to employees’ individual functions. For example, the accountant has all the accounting information, the marketing person has all the marketing information, etc. In those cases, creating manual backups might be the only feasible option, unless the business is prepared to invest in an IT infrastructure that can support all devices.

**13. Remember that physical security is part of cybersecurity**

Physical IT assets represent a significant amount of risk. Connecting, disconnecting, rebooting, and loading are among the many actions that an attacker can take to facilitate or launch a cyber attack when they have physical access to business devices. Computers with the most sensitive business information should be kept in a safe location, like a

---

**CHECK CYBER HYGIENE**

Organizations need to identify appropriate cyber hygiene practices and policies. Admins can consider points 1–13 in this section of the guide and determine the most relevant guidance for the types of information and systems of the business. Additionally, they should consider whether the business is utilizing as much of this guidance as possible and then identify any areas for improvement and how to implement these updates.

---


26  When there is an incident, even if a business does regular backups, it always loses some of its data. If a backup is done daily at the close of business on Friday, and an attack happened at the end of a Monday, the gap would be 72 hours.


28  PC Magazine regularly reviews backup services and rates them according to different benchmarks. [https://www.pcmag.com/picks/the-best-online-backup-services](https://www.pcmag.com/picks/the-best-online-backup-services)
locked cabinet or office. A router should not be left unsecured in an open-access area. Businesses should be sure that industrial connected devices require keys to operate. To determine which devices are critical, at minimum, a business should know what devices it has, what they are used for, and the type of information that is stored on them.

Most businesses are likely to already have strong physical security protocols, and the measures required depend on the type of business and its location. The important point is to include cyber assets in the physical security of the business.

14. Explore the possibility of cyber insurance

In some markets, insurance companies offer policies that cover losses resulting from a cyber attack, like a network disruption or data breach. Cyber insurance should not be viewed as a replacement for good cybersecurity. Where available, this insurance can be a valuable tool to mitigate damage and to fortify cyber defenses, but it does not eliminate risk nor does it cover all the consequences and costs of cyber incidents or risks.

When making the decision about buying insurance and what kind, businesses need to consider its specific risk profile and not what other businesses have, even if they are similar. Take the example of a business that provides guaranteed on-time product delivery. If a cyber attack on that business prevents it from delivering the product on schedule, the business will have higher liability exposure than its competitors.

MITIGATING RISK: BUSINESS INSURANCE COVERAGE

Businesses with business insurance policies should contact their insurer to determine whether cyber attacks or losses triggered by a cyber incident, such as lost data because of theft by an employee, are covered. Organizations can also inquire about additional cyber coverage and whether, as part of the insurance policy, the insurer offers support for improving the policyholder’s cybersecurity practices. These services are sometimes offered to reduce an insurer’s risks. Businesses should keep in mind the following points when discussing coverage with an insurer and when considering the purchase of a policy:

- There are costs associated with data recovery, including staff time and the potential purchase of new equipment. Data can be considered an item of value, as well.

- An incident affecting business or data can happen within the business system, in a third-party system, or while data are in transit. Data in third-party providers’ systems might not be covered under a standard policy.

- Often foreign actors originate attacks. This can include government-sponsored or rogue groups with the aim to cause general chaos and disruption, not necessarily to damage a particular business. Businesses should understand which incidents, including “acts of God,” are covered and not covered under the policy.
• Attacks can affect the reputation of a business and involve legal liability. Legal, IT, and other professional services may be needed to manage the consequences. Businesses need to clarify and understand potential responsibilities for payment of fines and compensation and any other obligations that arise in the event of a cyber incident.

• When personal data are compromised, laws can require the business to provide immediate notification to affected persons and businesses, in addition to reimbursement of money lost and costs incurred, plus other restitution. Organizations should check whether these requirements are covered under the policy.

• Insurance companies have different guidelines about ransomware or other extortion payments. Organizations need to understand in advance the policy and the required procedures, especially what to do and not do in these instances. Different insurance companies can define cybersecurity-related terms in different ways. Businesses should understand what each company means by the terms they use.

• There are items or risks that cyber insurance will not cover, such as potential future losses or the cost of improving security systems. An organization must keep in mind that these expenses need to be covered in the event of an incident.

Considering these points, businesses need to review whether cybersecurity insurance is appropriate for them. If it is, the business recovery plan needs to include the steps to gather required information to file a claim under the selected cyber insurance policy.

15. Consider hiring an IT professional

The steps in this guide can help a business to develop a robust cybersecurity plan and help it navigate through growth, adjustments, and adoption of new technologies. At some point, it might be necessary to hire an IT professional for the business, either as a consultant or as an employee. In that event, small business owners and their staff can gain a fundamental understanding of cybersecurity through this guide, enabling them to choose the type of assistance that would be most valuable to the business.

Most important is to know the risks for the business, what can be done to reduce immediate risk, and how to plan to reach risk-reduction goals within business constraints. To reiterate, cyber is another operational risk that can have significant consequences for a business and its customers. Cybersecurity awareness can set a business on a path to improve. Transformation does not need to happen overnight. It can be planned so that incremental goals are periodically met over time. What is important is to establish a business culture that includes cybersecurity awareness, to know what the business is currently doing to address cyber risk, and what needs to be done to improve the organization’s cybersecurity.
WHEN A CYBERATTACK OCCURS

Admins should have a hard copy list of emergency contacts in case of a cybersecurity incident. They should make sure that these contacts do not depend on company email or phone service functionality. Additionally, the admin should check that each person knows his or her responsibilities in the event of a cyber incident.

If applicable, the admin can contact the company payment processor and collect any information that may be needed to have on hand for incident recovery.

CYBERATTACK PREPAREDNESS

Organizations can simulate a cyber incident to test the business’s response time and whether each employee knows his or her role. Use backups to practice restoring operations.

A business should always respond promptly in the event of a cyber attack or other cybersecurity incident. A quick reaction can be the difference between minor damage or major disruption of the business. First, an admin should notify the appropriate individuals. This could include internal staff with specific roles and identified external consultants who can perform specialized services that may be needed, such as securing operations, stopping a data breach, performing IT forensics, fixing vulnerabilities, crafting legal memoranda for reporting, and communications to appropriate authorities and stakeholders, such as customers and suppliers. They should determine necessary legal obligations based on the type of incident. Governments or government entities might regulate notification of security breaches differently, which is particularly true in cases where personal data are involved.

Restoring Operations

In a cyber event, it may be necessary to take computers and network equipment offline to prevent further access to the business systems and to avoid the spreading of malware to uninfected equipment.

Businesses should follow the advice of the company IT professional or antivirus and/or backup provider. Full system backups, as discussed above, are often the easiest and cleanest way to restore systems to their previous, unaffected state and to resume operations. Organizations need to be sure to identify the source of the attack so that the same vulnerability is not exploited again resulting in another compromise of business systems.

The exact steps to restore operations depend on the nature of the incident, business, and data involved.

Managing Communications Effectively

After a business has been the target of a cyber attack, the communication strategy should change to emergency mode. What is said publicly in the moment can be critical to surviving an attack, maintaining business trust and reputation, and minimizing legal liability. Carnegie Mellon University Software Engineering Institute has developed a Guide to Effective Incident Management Communications, which sets out how to approach communications during an incident. That guide also references communications to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), making them easier to integrate into other communications efforts.
Businesses should develop a communications plan by following the guide and Carnegie Mellon’s Top Ten Considerations for Effective Incident Management Communications.\(^\text{30}\)

Organizations should:

1. Consider communications as a strategic initiative.
2. Have a reactive communications plan in place.
3. Consider the company messaging, reputation, and stakeholders as critical factors in the development of communications plans.
4. In the communications plan, clearly define and determine the following key components:
   - Establish the purpose;
   - Determine the audience;
   - Define roles and responsibilities;
   - Understand and standardize the messaging;
   - Determine and establish communication channels; and
   - Determine methods of message distribution.
5. Continually train and test the plan. Be sure that the plan works, and as with the incident response plan, test it beforehand so it is ready for incident management.

Sharing information and communicating with the public and/or customers is appropriate in most scenarios, but it is important for businesses to liaise with local law enforcement and other relevant authorities before making public announcements. The method and content of communication varies depending on the scenario. Media management should also be considered because the news media could report the incident, making it important to understand the media’s incentives as well as those of the business, in addition to the alignment of the two.

**NOTIFY THE AUTHORITIES**

When Internet-related offenses, e.g., hacking, ransomware, etc., happen, acting promptly can help minimize the damage to the business and may limit legal liability if compliance issues are involved. Each jurisdiction has specific reporting requirements and time frames, so businesses should check with the local authorities before an incident occurs to know which requirements apply to the business. This includes the specific legal requirements and recommendations for when to involve the authorities if threats or ransom demands are received. Cyber offenses may be investigated and prosecuted differently from other crimes, so organizations need notify all the appropriate authorities that would have oversight over the incident. It is best to know this information ahead of time so key personnel are aware of reporting requirements.

In general, businesses should expect to provide accurate and complete information about the attack and the parties involved, including:

---

\(^{29}\) [https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=651816](https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=651816)

\(^{30}\) [https://insights.sei.cmu.edu/blog/top-10-considerations-for-effective-incident-management-communications/](https://insights.sei.cmu.edu/blog/top-10-considerations-for-effective-incident-management-communications/)
• The type of incident, when it was detected, and what happened.
• Whether financial transactions were involved, such as a ransom. Government agencies will likely require the numbers and names of the account holders, transaction dates and amounts, transaction destinations, etc.
• Copies of the communications between the attacker and the victim.
• Any other information that can be relevant to the reported hack, including name and contact information of businesses and individuals affected through exposure of their data.

Administrators should be aware that attackers use techniques which allow them to penetrate and remain in a network undetected until launching an attack. Thus, there can be a time gap between when initial breach and the illegal activities that take place. For instance, access to a network’s most critical business data may be breached, but the business may not know about it until later, when customers call about unauthorized charges to their credit cards. Organizations should be sure to document all the circumstances and their timelines for a complete record of the incident. This could include logins to the network, traffic logs, Internet Protocol (IP) addresses, websites involved, electronic orders to perform transfers, etc. An IT professional can help gather all this information. When in doubt, businesses should add the information to the incident record. Seemingly unimportant information could be crucial, especially when all the circumstances are considered. If an IT professional is engaged, he or she should also verify that the attacker is no longer present in the network. The IT professional should liaise with the authorities regarding investigation of the incident and preservation of evidence.

NOTIFY SERVICE PROVIDERS

Recent attacks have followed a “hub-and-spoke” model, as attackers breach systems developed by providers to target their clients. If the incident involves service providers, such as the business payment processor, to make unauthorized payments or a provider’s facility where data are stored, businesses should notify them and work together in consultation with the authorities to mitigate the damage and expedite recovery. Similarly, a business might be part of supply chains and the cyber incident might have exposed the chain in whole or in part. Organizations should notify both downstream and upstream partners about the incident and should share relevant information.

Administrators should discuss these plans with service providers and suppliers as part of the preparation before an attack so that everyone knows the process to report an incident, the information needed to get support, and how to restore operations. They need to document that process as part of the business’s cybersecurity strategy.

NOTIFY CLIENTS AND CUSTOMERS

Timely and candid disclosure, in addition to following expert advice and coordinating with the authorities, can help assure all those affected that their interests are being protected and that the immediate and long-term impacts of the incident are being minimized.
Notifications usually need to meet legal or regulatory requirements. When first notifying the authorities, businesses need to ask whether laws or regulations mandate a specific way to notify affected parties, the characteristics of those notifications, and the time frame for doing so. It is important that interactions do not compromise any investigations by the authorities, making their involvement in the timing and content of the organization’s communications crucial.

Businesses should consider including the following information when developing communications:

- A simple and truthful explanation of the incident;
- An explanation of the data that was compromised and how the breach can affect clients/customers and suppliers now and in the foreseeable future;
- Reference to applicable laws or regulations and agencies involved in the case;
- What actions are being taken to recover from the incident and to protect customers’/clients’ and suppliers’ interests;
- Advice on what customers/clients and suppliers can do to protect themselves if their data has been compromised or misused;
- A point of contact from the business to answer questions;
- Means by which clients/customers and suppliers will be kept informed of developments (e.g., via email, on the business website, etc.), following legal requirements as applicable.

**SOCIAL MEDIA**

Organizations should assume that the incident will be shared on social media. The communications plan should include a component on how to effectively utilize social media. The same points described above apply to social media communications, but anything posted to social media is likely to become public—beyond the group of affected customers/clients or suppliers.

**Learning from the Incident**

After normal operations are restored, businesses should take stock of what happened, what the attackers were able to access, and how effectively the response plan worked. Then organizations can review the security measures in place and look for methods to strengthen them to help prevent a similar attack from happening again, as well as any other types of attacks for which the business is unprepared. (See “Categories of Threats,” in Part I of this guide). They should consider whether there is anything that could be done in the future to improve a response, thinking about how the breach was discovered, how it was communicated both internally and externally, and how it was resolved. It might also be easier to plan for future incidents with more accurate knowledge of the costs (financial, reputational, and operational, among others) of an attack to the business and which measures are worthwhile to help prevent one.

**CREATE PROACTIVE COMMUNICATIONS**

Businesses should draft the template of the initial message to consumers/clients and suppliers in the event of a cybersecurity attack that exposes their data. They need to tailor this message to the kinds of customer/client and supplier data collected and stored in the business and to ensure that it complies with applicable legal requirements.

**MAKE HARD COPIES**

Using the information compiled in following this guide, organizations should prepare a cybersecurity emergency folder containing hard copies of all documents prepared for cyber mitigation and eventualities. They need to ensure that the folder is accessible if computer systems are unusable in the event of a cyber incident.

**CAPTURE LEARNING**

After every incident and at least once a year, organizations should revise and further develop the business response plan and staff training to document what has been learned and any changes that should be implemented.
CONCLUSION

The steps outlined in this guide generally do not require a high level of expertise or a large expenditure of funds, but they do need thought and planning to put into action. Although these are basic, low-cost actions that a small business can implement, the steps can be integrated with more sophisticated strategies as the organization matures in its understanding of cyber and as the business grows. As cyber technology develops and further evolves, new threats will emerge and new resources for businesses will become available. In the meantime, the aspects covered in this guide provide a solid basic approach and plan for building cybersecurity and resilience into a small business.