Cyber

Information Security and Cyber Infrastructure Self-Assessment

In today's technology-driven world, cyber threats represent a critical and growing risk. The loss of sensitive information has caused companies of all sizes to face reputational harm, loss of confidential data, and monetary losses for cleanup and regulatory fines. At CNA, we understand that businesses must stay ahead of emerging cyber risks and the security threats they pose. That's why we provide consultative support, coverage, and risk control services for privacy and data protection. For businesses, the key to safeguarding information starts with security.

This checklist is an assessment tool based on the principals of the CNA CyberPrep risk management program and the National Institute of Standards and Technology (NIST) Framework for small and medium businesses. Each question is identified by the corresponding section (i) of the NIST Guide, which you can use for further guidance. The results of the assessment help to identify security control gaps and create baselines to address the potential impact of loss prevention and mitigation efforts.

		Yes	No	NA
1	Have you identified the level of Risk the Threats (Environmental, Business Resources, and Hostile Actors), Likelihood, and Impact of a data security incident create?	○	○	○
2	Have you identified the paper, electronic, and other records, computing systems, and storage media including laptops, mobile phones, and portable devices that contain sensitive information?	○	○	○
3	Do you have a policy in place not to leave your laptops, phones or other devices unattended in public, even locked in a car?	○	○	○
4	Do you conduct full, nationwide, criminal background check, sexual offender check, and if possible a credit check on all prospective employees?	○	○	○
5	Do you set up a separate account for each user (including any contractors needing access)?	○	○	○
6	Do you enforce a company policy governing security, privacy and acceptable use of company property that must be followed by anyone who accesses your network or sensitive information in your care?	○	○	○
7	Do you enforce a strong/complex password policy of at least 8-20 characters?	○	○	○
8	Do you physically and electronically limit access to sensitive information on a need –to-know basis and revoke access privileges upon a reduction in an individual's need to know?	○	○	○
9	Do you enforce a "clean desk" and "clear screen" policy in which sensitive information must not be accessible or visible when left unattended?	○	○	○
10	Have you installed electrical surge protectors and UPS (uninterruptible power supply)?	○	○	○
11	Do you check for security patches to your systems at least weekly and implement them within 30 days?	○	○	○
12	Have you installed firewalls between your internal network and the Internet?	○	○	○
13	At least once a year, do you provide security awareness training for everyone who accesses your network or sensitive information in your care?	○	○	○

		Yes	No	NA
14	On your wireless networks; do you use security at least as strong as WPA2 authentication and encryption, and do you require two factor authentication (access token and password/account logon) before allowing wireless connections to your network? (Answer NA ONLY if you do not use wireless networks.)	○	○	○
15	Do you require multi-factor authorization when your network is accessed remotely and/or when cloud resources are utilized?	○	○	○
16	Do you replace factory default settings to ensure your information security systems are securely configured? This would also include changing router default names, changing router default passwords, turning off remote management features, and ensuring administrator access is logged out of regularly.	○	○	○
17	Do you encrypt all sensitive records and files that are held at rest and/or transmitted across public networks, and that are to be transmitted wirelessly?	○	○	○
18	At time of hire and at least once a year, do you provide security awareness training for everyone who accesses your network or sensitive information in your care?	○	○	○
19	Do you have up-to-date versions of system security agent software (including malware, antivirus, and firewall protection) and reasonably up-to-date (within 30 days) security patches and virus definitions?	○	○	○
20	Do you have monitoring in place to alert you to the occurrence of unauthorized use of or access to sensitive information?	○	○	○
21	Do you have a written procedure that you rehearse at least yearly to ensure that you are proficient in responding to and recovering from network disruptions, intrusions, data loss and breaches of the following types: a. Network attacks and incidents (including: malicious code, hacking, spyware)? b. Breaches of privacy/confidentiality? c. Denial of service attacks?	○	○	○
22	Do you back-up your network data and configuration files daily and store back-up files in a secure location, and rehearse your procedure for restoring from back-ups at least yearly?	○	○	○

Once you have completed your data security assessment, you should now have a better understanding of potential threats and vulnerability areas. Using the answers to these questions will help you prioritize your risk mitigation efforts. Make sure you include key stakeholders in the self-assessment process. The self-assessment should be repeated at least annually and when business conditions change. For more information on data security protection and controls, please refer to our list of reputable resource websites that can help you achieve a more secure cybersecurity framework.

Additional Resources

National Institute of Standards and Technology
Small Business Information Security: The Fundamentals
(free download)

Federal Trade Commission – Protecting Small Businesses
FTC.gov/SmallBusiness

Center for Internet Security – Critical Security Controls
https://www.cisecurity.org/controls/

CNA Risk Control – Click on Property, Assets & Products then Cyber Liability
www.cna.com/riskcontrol

Small Business Information Security: The Fundamentals, Rev. 1,
https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7621r1.pdf
(last visited May 9, 2019)

For more information, visit cna.com.

1. Have you identified the level of risk the threats (environmental, business resources, and hostile actors), likelihood, and impact of a data security incident create?

Threat Level Risk

In information security, a threat is anything that might adversely affect the information your business needs to function. These threats may come from personnel or natural events; they can be accidental or intentional acts. Some of the most common information security threats include:

- Environmental (e.g. fire, water, tornado, earthquake)
- Business resources (e.g. equipment failure, supply chain disruption, employees)
- Hostile actors (e.g. hackers, hacktivists, criminals, nation-state actors)

When looking at these various threats, many people do not understand how they relate to information security. It is helpful to consider what would happen in the event of, for example, a flood. Computers, servers, and paper documents can easily be destroyed by even a small amount of water. If it is a large flood, you may not be allowed in the area to protect or collect the information your business needs to run.

2. Have you identified the paper, electronic, and other records, computing systems, and storage media including laptops, mobile phones, and portable devices that contain sensitive information?

Identify Sensitive Information Sources

Because it may be unreasonable to expect to protect every piece of information your business uses against every possible threat, it is important to identify what information is most valuable to your business (or to others). This first step is often the most challenging and most important part of risk management.

Start by listing all types of information your business stores or uses. Define "information type" in any useful way that makes sense to your business. You may also want to have your employees make a list of all the information they use in their regular activities. List everything you can think of, but you do not need to be too specific. For example, you may keep customer names and email addresses, receipts for raw material, your banking information, or other proprietary information.

3. Do you have a policy in place not to leave your laptops, phones or other devices unattended in public, even locked in a car?

Hardware Device and Information Security Policies

Companies should implement policies and procedures to identify acceptable practices and expectations for their business operations, to train new employees on their information security expectations, and to aid investigations of incidents. These policies and procedures should be readily accessible to employees – such as in an employee handbook or manual.

The scope and breadth of these policies is largely determined by the type of business and the degree of control and accountability management desires. Have a legal professional familiar with cyber law review the policies to ensure they are compliant with local laws and regulations.

Policies and procedures for information security and cybersecurity should:

- Clearly describe expectations for protecting information and systems;
- Be acknowledged via employee signature;
- Make employees aware of penalties;
- At minimum, be reviewed annually; and
- Be communicated to all employees and staff.

4. Do you conduct full, nationwide, criminal background checks, sexual offender checks, and if possible, credit checks on all prospective employees?

Employee Background Checks

Perform complete nationwide, criminal background checks, sexual offender checks, and (where and to the extent permitted by law) credit checks on all prospective employees, especially if they will be handing your business funds. You can request one directly from the FBI or an FBI-approved channeler.

- Additional background steps:
- Conduct a check on yourself and your leadership team
- Where applicable, validate educational background
- Conduct reference checks

5. Do you set up a separate account for each user (including any contractors needing access)?

User Access Policies

Set up a separate account for each user (including any contractors needing access) and require that strong, unique passwords be used for each account. Without individual accounts for each user, you may find it difficult to investigate data loss or unauthorized data manipulation. Ensure that all employees have minimal access needed to complete typical work functions and that their accounts do not provide administrative privileges unless absolutely necessary. This will hinder any attempt— intentional or not—to improperly access sensitive data, copy or transmit confidential information, or install unauthorized software. Consider using a guest account with minimal privileges (e.g. internet access only) if needed for your business.

6. Do you enforce a company policy governing security, privacy and acceptable use of company property that must be followed by anyone who accesses your network or sensitive information in your care?

User Hardware Device and Information Security Policies

Companies should implement policies and procedures to identify acceptable practices and expectations for their business operations, to train new employees on their information security expectations, and to aid investigations of incidents. These policies and procedures should be readily accessible to employees – such as in an employee handbook or manual.

7. Do you enforce a strong/complex password policy of at least 8-20 characters?

Password Strength

Good passwords consist of a random sequence of letters (upper case and lower case), numbers, and special characters, and are at least 12 characters long. Policies should discourage the reuse of passwords on multiple systems or accounts because a breach of one may lead to a breach of the other. Use of password managers to create and store multiple strong passwords may be appropriate in some circumstances.

Password policies also should apply to computers and devices which employees use to access company data and applications. For example, employees may instruct the browser on their device to "remember" or "autofill" the password for company email or other applications. Unless the device is protected by an equally-strong password, any unauthorized user who accesses that device may be able to bypass the strong password.

For systems or applications that have important information, use multiple forms of identification (called multi-factor authentication). For example, when a user logs in with a password, they may also be sent a text message containing a code they have to enter to confirm their identity.

Biometrics (e.g. fingerprint scanners) and other devices may also be used, but they can be expensive and difficult to install or maintain.

8. Do you physically and electronically limit access to sensitive information on a need-to-know basis and revoke access privileges upon a reduction in an individual's need to know?

Employee Access Limits

Where possible, do not allow any employee to have access to all of the business's information or systems. Allow employees to access only those systems and specific information they need to do their jobs. Likewise, do not allow a single individual to both initiate and approve a transaction (financial or otherwise). This includes executives and senior managers.

Insiders – employees or others who work for a business – are a main source of security incidents. Because they are already known, trusted, and have been given access to important business information and systems, they can easily harm the business (deliberately or unintentionally).

Unfortunately, these types of events can be difficult to detect, so protecting against them is very important.

When an employee leaves the business, ensure they no longer have access to the business's information or systems. This may involve collecting their business ID, deleting their username and account from all systems, changing any group passwords or combination locks they may have known, and collecting any keys they were given.

9. Do you enforce a “clean desk” and “clear screen” policy in which sensitive information must not be accessible or visible when left unattended?

Clean Desk/Clear Screen

Determine who has or should have access to your business’s information and technology. Include whether or not a key, administrative privilege or password is required. To help collect this information, review your list of accounts and what privileges those accounts have.

Be aware of anyone who has access to your business. Do not allow unknown or unauthorized persons to have physical access to any of your business computers. This includes cleaning crews and maintenance personnel. Do not allow computer or network repair personnel to work on systems or devices unsupervised. No unrecognized person should be able to enter your office space without being questioned by an employee. If a criminal gains physical access to an unlocked machine, they can relatively easily steal any private or sensitive information on that machine.

Physically lock up your laptops and other mobile devices when they are not in use.

Varying levels of security policies may be required depending on the nature and location of the computer. For example, unsupervised computers in public areas (e.g., information kiosks, retail terminals) probably require more security precautions than supervised computers in public areas (e.g., notebook computers which employees use in airport terminals or coffee shops) or desktop computers used by employees in secure company offices.

10. Have you installed electrical surge protectors and uninterruptible power supply (UPS)?

Electrical Interruptions

Surge protectors prevent spikes and dips in power from damaging your electronic systems, which can cause data loss or work interruption. Extension cords and "power strips" are not synonymous and do not necessary protect against electrical surges.

Uninterruptible power supplies (UPS) provide a limited amount of battery power to allow you to work through short power outages and provide enough time to save your data when the electricity goes off. A UPS usually provides surge protection as well. They come in varying sizes intended for individual computers, banks of multiple computers, or event whole facilities, and they are especially useful for desktop computers, servers, and mission critical, always-on hardware like network switches, routers, and modems. Make sure the size and type of UPS is sufficient to meet the needs of your particular business.

Ensure each of your computers and critical network devices are plugged into a UPS. Plug less sensitive electronics, or devices like notebook computers which already have their own battery, into surge protectors. Test and replace UPS and surge protectors as recommended by the manufacturer.

11. Do you check for security patches to your systems at least weekly and implement them within 30 days?

Security Patches

Any software application – including operating systems, firmware, or plugins installed on a system – could provide the means for an attack. Only install those applications that you need to run your business and patch/update them regularly. Reputable hardware manufacturers and software vendors should provide patches and updates to their supported products to correct security concerns (and sometimes to improve functionality). Ensure that you know how to update and patch all of the software and firmware on each device you own or use.

When you purchase new computers, check for updates immediately. Do the same when installing new software. You should only install a current, vendor-supported version of software or firmware you choose to use.

Vendors are not required to provide security updates for unsupported products. For example, Microsoft ended support for Windows XP on April 8, 2014 and no new patches will be provided for that operating system, even though it has known vulnerabilities [Msoft WLFS].

It may be useful to assign a day each month to check for patches. There are products which can scan your system and notify you when there is an update for an application you have installed. If you use one of these products, make sure it checks for updates for every application you use. You can check for updates directly with the original manufacturers of the applications you have installed.

12. Have you installed firewalls between your internal network and the internet?

Network Firewalls

Firewalls can be used to block unwanted traffic such as known malicious communications or browsing to inappropriate websites, depending on the settings. Install and operate a hardware firewall between your internal network and the internet.

Firewalls take many forms. They can be freestanding network appliances, or they can be implemented by your wireless access point/router or the cable or fiber modem provided by the Internet Service Provider (ISP) of the small business. There are many hardware vendors that provide firewall wireless access points/routers, firewall routers, and separate firewall devices. Ensure that the firewall is patched regularly with the manufacturer's software and firmware updates, and install antivirus software on the firewall where applicable.

Most computer operating systems offer a software firewall which may be an important adjunct to a hardware firewall, especially for notebook computers and other portable devices.

13. At least once a year, do you provide security awareness training for everyone who accesses your network or sensitive information in your care?

Employee Training

Train employees immediately when hired and at least annually thereafter about your information security policies and what they will be expected to do to protect your business's information and technology. Ensure they sign an agreement stating that they will follow your policies, and that they understand the penalties for not following your policies.

Train employees on the following:

- Approved uses of business computers and mobile devices
- Managing customer and business information
- Security and incident response
- Best practices

Additional training resources:

- Local Small Business Development Center (SBDC), SCORE Chapter
- Community or technical colleges
- Commercial training vendors
- The Small Business Administration (SBA)
- Federal Trade Commission (FTC)

14. On your wireless networks; do you use security at least as strong as WPA2 authentication and encryption, and do you require two factor authentication (access token and password/account logon) before allowing wireless connections to your network? (Answer NA ONLY if you do not use wireless networks.)

Wireless Network Security

Recommended actions and settings for wireless networking

- Change the administrative password that was on the device when you received it, and give it a new "strong" password (see #7 above).
- Disable broadcasting the Service Set Identifier (SSID)
- Set router to use Wi-Fi Protected Access 2 (WPA-2), with the Advanced Encryption Standard (AES) for encryption. Do not use WEP (Wired-Equivalent Privacy) as it is not considered secure.

Additional considerations:

- Establish separate wireless internet access for customers and business resources
- Access only trusted proprietary wireless access points
- Avoid connecting to unknown or unsecured/guest wireless access points unless the device implements an encrypted virtual private network (VPN).

15. Do you require multi-factor authorization when your network is accessed remotely and/or when cloud resources are utilized?

Multi-factor Authentication

Multi-factor authentication (MFA) is a redundant identification process which requires users to utilize multiple verification steps to gain access to a network or system. The authentication process can entail a combination of passwords, texts, biometrics or other verification methods.

16. Do you replace factory default settings to ensure your information security systems are securely configured? This would also include changing router default names, changing router default passwords, turning off remote management features, and ensuring administrator access is logged out of regularly.

System Default Settings

Many network devices, routers, access points (AP), repeaters, and modems come from the manufacturers with commonly known default settings which make these devices easily accessible.

These default settings should be immediately changed to avert unauthorized access by bad actors locally or via the internet.

Additionally, many network-aware devices come with certain security features disabled in order to permit use of certain features (e.g., universal plug and play, remote management). If these features are not needed for business purposes, disable them and restore stronger security settings.

17. Do you encrypt all sensitive records and files that are held at rest and/or transmitted across public networks, and that are to be transmitted wirelessly?

File Encryption

Encryption is a process of making your electronically stored information unreadable to anyone not having the correct password or key*.

Use full-disk encryption—which encrypts all information on the storage media – on all of your computers, tablets, and smart phones. (Many systems come with full-disk encryption capabilities, but not all mobile devices provide this capability.) Properly used, encryption reduces the likelihood that a bad actor can access your confidential data, even if they get access to your systems and files.

Email is inherently insecure, so consider encrypting all confidential or proprietary files you send across the public network.

* NIST SP 800-101 Rev. 1, Guidelines on Mobile Device Forensics, defines encryption as “Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data” [SP800-101].

18. At time of hire and at least once a year, do you provide security awareness training for everyone who accesses your network or sensitive information in your care?

New Hire Training

Train employees immediately when hired – and provide updates and refreshers at least annually thereafter – about your information security policies and what they will be expected to do to protect your business's information and technology. Ensure they sign an agreement stating that they will follow your policies, and that they understand the penalties for not following your policies.

Provide training on:

- Approved uses of computer and mobile devices
- Managing customer and business data
- Incident response
- Working safely and securely

19. Do you have up-to-date versions of system security agent software (including malware, antivirus, and firewall protection) and reasonably up-to-date (within 30 days) security patches and virus definitions?

Security Software Updates

Malware (short for Malicious Software or Malicious Code) is computer code written to do unauthorized things on the systems where they are installed: often to steal or harm. It includes viruses, spyware, and ransomware.

Malware comes in many forms. Sometimes it pretends to provide a useful service (e.g. a browser search bar extension or weather applet), but Malware also can deplete computing resources (e.g. memory), change system security settings so the Malware can serve up advertisements, redirect users to unsafe websites, or install other software, and sometimes it can actively record your actions, steal passwords, or send your personal and sensitive information to cybercriminals.

- Install, use, and regularly update anti-virus and anti-spyware software on all business computers and mobile devices
- Configure automatic updates of anti- virus and anti-spyware software
- Make software available to employees who use personal computers and devices to conduct company business
- Consider utilizing two different anti- virus solutions and vendors to improve virus detection capabilities

20. Do you have monitoring in place to alert you to the occurrence of unauthorized use of or access to sensitive information?

Incident Monitoring and Alerts

Protection / detection hardware or software (e.g. firewalls, network routers or switches, anti-virus) often has the capability of keeping a log of activity. Ensure this functionality is enabled (check the operating manual for instructions on how to do this). Logs can be used to identify suspicious activity and may be useful in post-event forensic investigations.

- Regularly back up log files
- Save log files for minimum of one year. Some industries or lines of business may have more substantial requirements for data.
- Consider having a cybersecurity professional review the logs for any unusual or unwanted trends, which may indicate a more serious problem or signal the need for stronger protections in a particular area

21. Do you have a written procedure that you rehearse at least yearly to ensure that you are proficient in responding to and recovering from network disruptions, intrusions, data loss and breaches of the following types:

a) Network attacks and incidents (including: malicious code, hacking, spyware)

b Privacy/confidentiality breaches

c) Denial of service attacks

Incident Response

Develop a plan for what immediate actions you will take in case of a data breach, fire, medical emergency, burglary, or natural disaster.

The plan should include the following:

- Roles and responsibilities
- Information system and data containment plan
- Contact notification plan – cybersecurity, emergency personnel, senior executives, legal professional, public relations agency, insurance providers and potentially federal law enforcement
- Customer notifications in accordance with all local, state and federal laws
- Outline the factors and parameters, which define various types of information security and data breach events

22. Do you back-up your network data and configuration files daily and store back-up files in a secure location, and rehearse your procedure for restoring from back-ups at least yearly?

Network Data Backups

Conduct an automatic incremental or differential backup business computers and mobile devices at least once a week. This type of backup only records any changes made since the last backup. In some cases, more frequent backups are necessary with higher data volume creation or higher risk exposure associated with data loss. Many security software suites offer automated backup functions.

These backups should be stored on:

- Removable media (e.g., external hard drive)
- A separate server that is isolated from the network
- Online storage (e.g., a cloud service provider)