**22 Best Items for a Cybersecurity Checklist**

By [**George Mutune**](https://cyberexperts.com/author/georgemutune) 8/28/22

A [cybersecurity](https://cyberexperts.com/encyclopedia/cybersecurity/) checklist is important since cybersecurity investments can be a complicated process. An organization must first identify vulnerable assets, determine how vulnerable they are, and allocate sufficient budgets needed to enhance their security. In any cybersecurity program, companies should, at the very least, include the following:

1. **Procedures for identifying and assessing cybersecurity threats and risks**
2. **Secure assets from attempted cyber intrusions**
3. **Detect instances of IT assets and systems being compromised**
4. **Plan a response in anticipation of a data breach or security compromise**
5. **Plan and implement a recovery plan for recovering unavailable, stolen, or lost assets**

Developing a holistic program means covering all IT assets and information systems. For organizations with vast software, hardware, or network products, it can be challenging to develop an all-rounded cybersecurity program. This necessitates the use of a cybersecurity checklist. A cybersecurity checklist lists items that must be protected. It identifies and documents a set of cybersecurity procedures, standards, policies, and controls. The following sections discuss important items that must be included in a cybersecurity checklist.

**Overarching best security practices**

All organizations should identify the best security practices when accessing or handling sensitive data and critical information systems. The following three items are essential to maintaining a useful cybersecurity checklist.

**1.  Documented Policies**

Documented policies list the security guidelines and obligations of employees when interacting with company systems or networks. The policies enable an organization to ensure employees, third parties, or managed service providers observe minimum but mandatory security measures. Common policies to include in a cybersecurity checklist include acceptable use, internet access, email and communication, remote access, BYOD, [encryption](https://cyberexperts.com/encyclopedia/encryption/) and privacy, and disaster recovery.

**2.  Acceptable use Policy**

A cybersecurity checklist should include an acceptable use policy. Acceptable use consists of various rules that govern the use of an organization’s IT assets or data. The policy is crucial since it prevents system users from participating in practices that can impact the cybersecurity of an organization. All new users, which might be employees, third parties, and contractors, must accept to have read and understood the stipulated rules. This is before being allowed to access company networks and computer systems. By acknowledging to understand the policy, users agree to use information systems according to the organization’s minimum-security recommendations. As such, a business can be assured that user activities will not introduce [security risks and threats](https://cyberexperts.com/cybersecurity-threats/).

**3.  Internet access policy**

The internet has become ingrained in the daily activities of most individuals. People use the internet for research, accessing cloud services, and communicating through emails or social media platforms, among others. However, the same internet can be the downfall of an organization due to various reasons. For instance, cyber actors use the internet to deliver [malware](https://cyberexperts.com/encyclopedia/malware/). They can place malware on a specific website such that any user who visits it downloads and installs the malware. Such and other attacks executed through the internet are frequent. Therefore, a cybersecurity checklist should include a policy governing internet usage within an organization. Internet access policy contains guidelines regarding how users can access and interact with the internet. For instance, an internet access policy can prohibit users from visiting specific websites, or the frequency with which they can access social media platforms. This can facilitate the adoption of bolstered and strengthened cybersecurity postures.

**4. Emails and communication policy**

Emails are used for both internal and external communication. All employees in an organization must, therefore, have an email account. Emails are also an attacker’s preferred mode of delivering [phishing](https://cyberexperts.com/encyclopedia/phishing/) malware. Hackers send emails in batches to multiple targets hoping that one will click on the links or attachments containing malware. A policy regarding email usage can enable a company to prevent phishing attacks, thus improving the security of its data and systems. Such a policy can include rules requiring employees not to open emails sent by unknown people. Also, it can require that all incoming emails be scanned to detect malicious attachments or links with hidden malware. Additionally, an email and communications policy should require employees to avoid using personal emails when communicating work-related data. Such policies are essential to ensuring organizational security and should, therefore, be included in a cybersecurity checklist.

**5.  Remote access policy**

More businesses are adopting cloud technologies. This is to enhance their data collection and processing techniques and to improve employee productivity. Since cloud services are becoming more ingrained in running daily business operations, a cybersecurity checklist must contain a remote access policy. Remote access policies provide the necessary security requirements users should consider when accessing cloud accounts remotely. The cloud permits users to access data and other services from any location and device. This means that they can opt to work remotely outside the office. A remote access policy ensures that they observe secure practices when accessing sensitive information. For instance, the policy can require employees to use a VPN when accessing through a public and insecure internet network.

**6.  Bring Your Own Device (BYOD) policy**

Internet of Things has proliferated in recent years, leading to increased use of internet-enabled devices. The trend has seen most employees prefer using personal devices such as smartwatches, laptops, smartphones, and tablets to accomplish their assigned duties. This results in increased risks since the more the devices in use, the more the number of entry points a hacker can choose from. That notwithstanding, users may be unable to identify vulnerabilities present in their devices. Connecting to a corporate network or accessing data using vulnerable devices threatens their integrity, confidentiality, and availability. A BYOD policy enables an organization to manage the use of personal devices within a work environment, thus alleviating risks that can impact its overall security. A BYOD policy can include requirements such as employees only connecting to the corporate network using devices provided by the organization.

A [BYOD policy](https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating) should be updated frequently to ensure it covers all emerging technologies. Including a BYOD policy in a cybersecurity checklist facilitates the secure usage of personal devices, thus protecting an organization from multiple threat sources.

**7.  Encryption and privacy**

Sometimes, cyber adversaries manage to bypass the most secure networks and systems. As such, organizations are not fully guaranteed that their data and classified information are 100% secure. An encryption and privacy policy should hence be a requirement in all processes where users interact with organizational data. The encryption and privacy policy should require users to encrypt all data, whether it is at rest or in transit.

Encrypting data provides an additional security layer to the encrypted information if cyber adversaries manage to breach the adopted cyber defenses. Moreover, the policy should include the preferred encryption technique to ascertain that all users use the same level of standard encryption techniques. Encryption should be included in all cybersecurity programs and checklists since it is the simplest method for preserving data integrity, confidentiality, and availability.

**8.  Disaster recovery policy**

As previously stated, adopting the most powerful security solutions do not guarantee that an organization is entirely secure. In anticipation of the occurrence of a cyber-attack, businesses should maintain effective disaster recovery policies. A disaster recovery policy contains a set of actions that different users should undertake to recover from an attack. Developing effective disaster recovery policies can facilitate a company’s efforts to contain an attack.

Also, by maintaining and continuously updating a disaster recovery policy, a business assigns its employees the roles to complete to ensure a speedy recovery of critical data, networks, or computer systems. The policy further addresses the communication channels to ensure that the involved personnel has seamless communication during the entire time of a disaster recovery process. A disaster recovery policy should, therefore, be at the heart of all cybersecurity checklists.

**9.  Modern and updated software**

Every business should consider including the use of modern software programs in its cybersecurity checklist. Acquiring up-to-date software is vital to enhancing the security of an organization. This is because modern software programs are developed to be resilient against current risks and attacks. Using legacy operating or software systems introduces various security challenges. They might be containing unaddressed vulnerabilities, or their vendors might have stopped supporting them in releasing security updates and patches. Using current software does not necessarily mean that it is entirely secure.

Vulnerabilities emerge all the time, and failing to address them can provide hackers with a playing ground for exploiting the vulnerabilities. As such, a cybersecurity checklist should include a patch management program. Software or hardware vendors release security patches to mitigate vulnerabilities as they occur. Regularly applying security patches can help protect an organization from cyber-attack incidences.

**10.  Frequent employee training**

More than 90% of the cyber incidences are caused by erroneous user mistakes or cybersecurity ignorance. For example, an employee leaving a computer without locking can result in disastrous data breaches. For this reason, all organizations need to include frequent training and awareness campaigns in their cybersecurity programs. Training and awareness provide employees with skills for securely using organizational systems, data, and networks. It also ensures that they are capable of identifying security risks, managing them, and reporting them to the relevant personnel.

In this regard, an employee training program should train employees on how to secure their workstations, emails, cloud accounts, and other types of information systems. Also, a training program should enable employees to understand how they can identify phishing emails and the actions they should undertake once identified. Such measures include marking the sender’s email address as [spam](https://cyberexperts.com/encyclopedia/spam/), reporting to IT, and alerting other employees of the attempted phishing attacks. There are other training items to be considered when developing an awareness and training program. These should be included to meet a company’s security needs.

**User security measures**

A practical cybersecurity checklist should contain measures that are specific to network and system users. The standards ensure that an organization remains protected whenever a user accesses the IT assets at his disposal. The following items need to be included in a cybersecurity checklist. This is to ascertain that user behaviors do not impact organizational cybersecurity.

**11.  Password etiquette**

Password etiquette refers to what consists of best password management practices. Passwords are often the most used defenses at all levels, and users must ensure that they observe best password practices. An essential password security requirement is users should always create robust passwords. The guidelines to consider include combining different characters such as numbers, alphabetical letters, and special symbols. This is to minimize the possibility of cyber adversaries guessing the passwords.

Also, a business should require users to create lengthy passwords. Passwords with 6-10 characters can provide sufficient security. It is also crucial for users to frequently change and update their passwords. A rogue college might access stored passwords and use them for identity theft or other malicious activities. To ensure high password complexity, users should consider using passphrases. These are strings of different words required to access a system. These and other password requirements should be included in a cybersecurity checklist.

**12.  Auditing disabled accounts**

Work accounts such as email and cloud accounts can be disabled due to various reasons. These reasons can include employees being reassigned to new roles and responsibilities, or if an employee stops working in an organization. Auditing disabled accounts allow a system administrator to identify accounts that are no longer in use. Disabled accounts provide security risks since malicious actors can access them along with all permissions and privileges.

As such, they can gain system and data access while posing as legitimate users. An audit of all outdated accounts ensures that those no longer in use are closed and deleted. Including auditing disabled or outdated accounts in a cybersecurity checklist enable a company to close all loopholes that can give adversaries unauthorized access to protected systems and information.

**13.  Preventing shared passwords and accounts**

Preventing users from sharing the same passwords or work accounts should be a priority for any cybersecurity program or checklist. Allowing users to share work accounts and passwords can result in highly impactful security risks. For example, it can be difficult to trace the user responsible for a security incident if it involves a shared account. Besides, allowing employees to share accounts and passwords encourages [insider threat](https://cyberexperts.com/encyclopedia/insider-threat/)s and attacks.

Employees participating in malicious activities can deny any accusations, pointing out that they are not the only ones with access to the account in question. Therefore, including the prevention of shared passwords and accounts as an item in a cybersecurity checklist can ensure a company audits all accounts. Subsequently, insider threats can be minimized, thus leading to enhanced cybersecurity.

**14.  Use of secure websites**

The use of secure websites, when connected to an organization’s network, should be a mandatory item in a cybersecurity checklist. Every business should require employees to only share organizational information or any sensitive data like passwords through secure websites. Secure sites have an HTTPS connection, which means that the connection is encrypted.

Encrypted connections allow secure data and information transfer, which is vital to ensuring that its integrity and confidentiality remain intact. Including the use of secure and encrypted websites in a cybersecurity checklist can enable a company to block users from accessing insecure websites. This eliminates instances where cyber incidences are as a result of the information being compromised through vulnerable sites. Such sites have an HTTP connection and as such, lack the necessary encryption schemes.

**Email security**

Almost all communication processes are done via email communication. Emails, however, provided the highest risks since they are a preference for delivering malware and [virus](https://cyberexperts.com/encyclopedia/virus/)es for most cyber actors. It is, therefore, essential for an organization to include email security in its cybersecurity checklist. The following are some of the points to consider in email security.

**15.  Filtering tools**

Email communication is the most widely used platform for executing phishing attacks and delivering malware. Phishing attacks are where cyber adversaries target multiple users with messages crafted to appeal to their interests. This is to trick them into clicking on a link or attachment that contains hidden malware. To ensure that such malware programs are caught before a user downloads them, businesses need to install tools for filtering all incoming messages. As such, they can detect embedded malware and prevent them from accessing the company’s networks or computer systems.

**16.  Email policy**

Developing and regularly updating an email policy should be included in a cybersecurity checklist. Emails can still be hacked without the knowledge of an organization, as email security is usually the responsibility of the email service provider. Documenting an email policy identifies the types of information that users are permitted or prohibited from sharing through emails. For example, an email policy can prevent users from sharing passwords, personal data, or financial information through emails.

**Website security**

Businesses use their websites for marketing their products and services. They also use emails to interact with customers by responding to inquiries or customer feedback. In some cases, some companies might collect a client’s personal information through their websites. Website security should, therefore, be an essential item in a cybersecurity checklist. There are two main points to consider to realize optimum website security.

**17.  SSL certification**

Companies need to obtain an SSL (Secure Sockets Layer) certification. An SSL-certified website means that it is secure, and it provides end-to-end encryption between a client and a server. By being SSL certified, a user can confidently transmit sensitive information without fearing that it will be intercepted and modified before it reaches the intended target. Moreover, an SSL-certified website not only means that users can access it and securely request or transmit information, but it also builds a company’s reputation. Customers prefer submitting their information through secure sites, and SSL certificate gains their confidence. As such, it is necessary to include SSL certification in a cybersecurity checklist.

**18.  Secure web hosting provider**

An organization should only seek the services of a secure web hosting provider. The key attributes to include in a cybersecurity checklist are the provider’s ability to isolate hosting accounts, mechanisms for regularly backing up the website, and the ability to maintain the server logs.

**Network security**

Ensuring [network security](https://cyberexperts.com/encyclopedia/network-security/) is crucial to any business. Cyber adversaries are always looking for exploitable network vulnerabilities to gain unauthorized access. The following items should be present in a cybersecurity checklist to realize maximum website security.

**19.  Powerful firewalls**

A network should be secured using powerful [firewall](https://cyberexperts.com/encyclopedia/firewall/)s. Combining several firewalls can provide enhanced network security. Protecting networks using a firewall facilitates the development of filtering rules in accordance with an organization’s security requirements. The rules are for filtering out incoming malicious connections that can affect the security of the network.

**20.  Password protection**

Maintain password security ensures only users with the correct permissions can connect to the network. A business should hence apply password security in its Wi-Fi routers to ensure only employees can access internal networks. To minimize the risk of a malicious user accessing the corporate network, a business should provide guests with a separate Wi-Fi network.

**21.  Network segmentation**

Network segmentation entails splitting a network into small but manageable segments. Network segmentation enhances both the security and performance of the network. In the event that a hacker accesses a part of a network, a segmented network can prevent the adversary from accessing other systems that are not connected to the same network. This is as opposed to an unsegmented network, where an adversary can move laterally, gaining access to all connected systems.

**22.  Automatic computer lock screens**

Computers should be equipped with an automatic lock screen functionality. They should be set to lock automatically, say after three minutes of inactivity. This is to prevent unauthorized users from accessing the computer and the network in extension.

**[George Mutune](https://cyberexperts.com/author/georgemutune)**

I am a cyber security professional with a passion for delivering proactive strategies for day to day operational challenges. I am excited to be working with leading cyber security teams and professionals on projects that involve machine learning & AI solutions to solve the cyberspace menace and cut through inefficiency that plague today's business environments.

**© 2022 CyberExperts.com. All Rights Reserved.**