

5 Common Cybersecurity Threats in 2022

Cost-Effective Solutions for SMBs



CurrentWare

Small-to-Medium businesses need to prioritize cybersecurity just as much as the big players.

Your employees are your greatest asset, but they can also become your greatest liability if they are not adequately trained on their cybersecurity risks and responsibilities.

If your employees aren't adequately equipped with the knowledge they need to use technology in the workplace safely they may inadvertently be putting sensitive data at risk.

This list serves as an essential checklist for teaching employees what they need to know to protect sensitive data against these five common threats.

The 5 Most Common Threats

- 1) USB Devices**
- 2) Social Engineering & Phishing Scams**
- 3) Stolen and Compromised Credentials**
- 4) Insider Threats**
- 5) Out-of-Date Security Patches**



1) USB Devices

Portable storage devices such as flash drives and external hard drives are useful tools for quickly and easily transferring data between computers, but they can also pose a significant security risk.

What is the danger?

- **Malware Infection:** Flash drives and other removable media can unknowingly transmit malicious software (malware) such as ransomware. Once an employee's computer is infected the malware can potentially spread to other computers within the network.
- **HID Payloads:** Human-interface-devices (HIDs) disguised as USB devices can execute a "payload" once plugged into the computer. The payload can be configured to give the attacker direct remote access to the employee's computer.
- **Data Loss:** If an unencrypted USB device with sensitive data is lost or stolen, that data is considered breached. Such an event could potentially lead to a customer having their identity stolen and the company facing serious non-compliance fines.

How to protect against this threat

- **Data Encryption:** When data and USB devices are encrypted the data on them cannot be accessed without a dedicated encryption key. Using encryption helps protect data by making it more difficult for bad actors to access the data on the device.
- **USB Blocker:** AccessPatrol's USB permission policies can enforce the exclusive use of authorized devices, preventing employees from transmitting data to personal external storage devices.
- **DLP Monitoring:** Monitoring file operations and peripheral device usage within the network provides IT security teams with the information they need to detect and mitigate unsafe data handling.
- **Training:** Employees need to be made aware of the dangers of unknown USB devices. They should be taught to never plug in a USB drive from an unknown source without first testing it on a computer that is disconnected from the network.



2) Social Engineering & Phishing Scams

Bad actors rely on the trust of employees to bypass your organization's security controls. According to [Verizon's 2020 Data Breach Investigation Report](#), social engineering was responsible for 33% of North American data breaches. The exact methods used to trick employees will differ; you'll need to establish clear policies and procedures for responding to unknown visitors and suspicious emails as they arise.

What is the danger?

- **Phishing:** Attackers will send either targeted or mass-distributed emails to employees that are designed to convince them to install a program or download a malicious attachment. The attachments can look like ordinary files such as Microsoft Word documents or PDFs, but they can contain executables that give threat actors direct access to your endpoint devices. Phishing attacks can convince employees to visit a website that downloads malicious software (*drive-by download*).
- **Vishing:** This method of attack is just like phishing emails, except it is done over the phone. Employees that are savvy about phishing may still place greater trust in phone calls, so it is important to emphasize that attackers may use this channel to steal information as well.
- **Social Engineering:** These attacks can use a variety of methods such as emails, phone calls, and even direct visits to your office to convince employees to give them access to confidential spaces and material.

How to protect against this threat

- **Spam Filter:** Email filtering & monitoring solutions can reduce the amount of malicious emails that make it into your employee's email inboxes.
- **Web Filter:** A web filter such as CurrentWare's BrowseControl can be used to proactively block access to websites that are known to contain malware and other web-based exploits.
- **Employee Training:** Your employees need to be provided with clear policies and procedures regarding their use of email. They must be taught how to spot a phishing email and what steps they should take once they discover a phishing email. Your organization must also set clear boundaries for what is and is not acceptable to share via email.



3) Stolen and Compromised Credentials

[The 2017 Verizon Data Breach Report](#) found that 81% of hacking-related breaches used either stolen and/or weak passwords. Stolen and compromised credentials can provide threat actors with direct access to your network, the sensitive data of your customers, and other mission-critical systems.

What is the danger?

- **Trusted Access:** If advanced security controls are not in place, stolen credentials can give bad actors unimpeded access to the company network.
- **Data Breach:** If the stolen or compromised credentials have direct access to sensitive files the hackers can easily exfiltrate that data and sell it for financial gain.
- **Damage Escalation:** Even low-level credentials can give an attacker the leverage they need to further exploit the network and compromise higher-level permissions.

How to protect against this threat

- **Password Hygiene:** Employees need to ensure they generate secure passwords that are easy to remember and difficult to guess. Each password should be unique to every account they create. To keep these passwords secure and inaccessible to outsiders they should store them in a password manager rather than leaving them written in a notepad that could be stolen.
- **Multi-Factor Authentication:** Traditional username & password credentials are too weak to use by themselves. Combining multiple methods of authentication such as hardware keys, one-time passwords, and local PINs that use a public-key cryptography model will make it more difficult for an attacker to use compromised credentials to infiltrate your network.
- **Reduce Admin Credentials:** Only a limited number of trusted users should be provided with admin credentials, and only if their role truly requires that level of access. As employees come and go these credentials need to be decommissioned to prevent “orphan accounts” from later being used in an attack.



4) Insider Threats

According to [Verizon's 2019 Data Breach Investigations Report](#) 34% of all breaches that happened in 2018 were caused by insider threats. The close contact insiders have to your organization's network provides a greater potential for them to cause significant damages.

Insider threats aren't always malicious. While you will absolutely need to have a plan for preventing jaded employees from loading company secrets on a flash drive and selling it to your competitors, more often than not insider threats are simply employees that are careless.

What is the danger?

- **Data Theft:** Trusted employees can maliciously abuse their privileges to steal valuable company data such as personally identifiable information (PII), financial records, and intellectual property.
- **Credential Theft:** Employees that are negligent about their data security responsibilities can accidentally leak their credentials by falling for phishing emails, fake login screens, and other attacks.
- **Vandalism:** Disgruntled employees can abuse their privileges to disrupt business operations by deleting critical files, destroying company equipment, or purposely leaking confidential data.

How to protect against this threat

1. **Employee Monitoring:** Collecting employee computer usage data helps IT security teams identify high-risk behaviors such as large file transfers, attempts to access unauthorized resources, and visiting potentially dangerous websites.
2. **Data Loss Prevention Software:** DLP software such as AccessPatrol can prevent privileged insiders from transmitting sensitive data to external storage devices.
3. **Block Cloud Storage:** Blocking access to cloud storage sites with a web filter will prevent negligent or malicious insiders from leaking sensitive data.
4. **Limit Access:** Employees should not be given access to more data or privileges than is truly necessary for their roles.



5) Out-of-Date Security Patches

Organizations that ignore critical security updates for applications, operating systems (OS), and other assets create an unnecessary data security risk. Businesses of all sizes need to ensure that all of the software and firmware used in their organization is frequently updated to prevent attackers from exploiting vulnerabilities.

What is the danger?

- **Zero-Day Vulnerabilities:** As never-before-seen (zero-day) vulnerabilities are discovered, vendors are quick to release critical security patches that protect their products against these exploits. Organizations that do not keep their assets up-to-date will remain vulnerable to these exploits until they've deployed the necessary patches.
- **Data Loss:** Attackers will use any available exploit they can find to bypass your network's security. Ignoring software updates provides them with an added opportunity to gain unauthorized access into your network to steal sensitive data.

How to protect against this threat

- **Automatic Updates:** Enabling automatic updates ensures devices are receiving the latest patches. Updates can be configured to occur outside of business hours to reduce disruptions.
- **Avoid Legacy Software:** When software reaches its "end of life" or "end of support" it is no longer receiving critical security updates. Avoid using operating systems and other software that is no longer being supported by their developers as they may not be secured against the latest vulnerabilities.
- **Remote Restart:** Manually restarting a fleet of computers is a time-consuming task. To make this critical step easier to manage, consider using a centralized power policy manager such as CurrentWare's enPowerManager to remotely restart computers.



More Resources

Resource	URL
Internet Usage Policy Template	https://www.currentware.com/internet-usage-policy-template/
Work From Home Policy Template	https://www.currentware.com/work-from-home-policy-template/
Removable Media Policy Template	https://www.currentware.com/blog/removable-media-policy-template/
How to Keep Data Safe When Offboarding Employees	https://currentware.com/how-to-keep-data-safe-when-offboarding-employees/
The CurrentWare Blog	https://www.currentware.com/blog/
Get a Free Trial of CurrentWare	https://www.currentware.com/download/

About CurrentWare

CurrentWare is a software company that provides a suite of workforce management solutions for computer monitoring, content filtering, data loss prevention, and remote power management.

CurrentWare's solutions are adopted by a wide array of government and private organizations including schools, hospitals, libraries, and for-profit businesses. CurrentWare customers improve their user productivity, data security, and business intelligence with advanced awareness and control over how technology is used in their organization.

For more information you can visit our website at www.CurrentWare.com

 AccessPatrol	Data loss prevention software to restrict and monitor USB device activity.
 BrowseControl	Content filtering software to restrict internet access and block the use of applications.
 BrowseReporter	Employee monitoring software that tracks website and application usage.
 enPowerManager	Remote device management software for configuring computer settings such as power states.