10 Best Cybersecurity Practices in 2022

Cybersecurity breaches are newsmakers. Such breaches can involve ransoms, weeks-long business outages, enormous inconveniences, and more, for your customers.

It costs money to ensure that your business data is secure. As new threats are always emerging, this cost becomes an ongoing expense, and a ROI is not always visible. But being lax on security could end up costing more if a breach puts your business continuity and reputation in danger. It could even put your customers' data in danger if a breach in your system provides access to theirs.

In the supply chain, cybersecurity requirements are increasingly driven by clients, business, insurers, industry standards and regulation. Advanced data security protocols are becoming a competitive edge and a consideration in the awarding of contracts.

Cybersecurity is a safety and security issue which is imperative for technology stability. This paper lists the top 10 cybersecurity best practices in 2022, compiled by CIFFA's Technology Committee based on information from multiple cybersecurity firms. The committee focused primarily on the needs of small businesses in the freight forwarding sector, keeping the resources of such businesses in mind.

Many of these practices require little financial investment for technology, but significant time to be properly implemented. While all are important practices, they do not all have to be implemented at once to increase security. Small freight forwarding companies should review the list and prioritize activities based on their current level of preparedness, requirements, and available resources.

1. Employ a risk-based approach to security

What:
Identify all valuable assets, document current state of cybersecurity protocols/tools and ensure accurate management on your security strategy. A thorough risk assessment will help prioritize security measures and make a strategy serve the corporate bottom line in the best way possible.

How:
Put yourself in the threat space and look at your own organization as an adversary would. Think about the campaign that they would run against you and how your controls align against that potential campaign.

2. Back up your data

What:
Ensure the security of your data by regularly backing it up. Backing up data is one of the information security best practices that has gained increased relevance in recent years. With the advent of ransomware, having a full and current backup of all your data can be a lifesaver.

How:
Ensure that the backup is thoroughly protected, encrypted, and frequently tested. If you backup to tape, ensure to store it off-site in a secured location, otherwise, use available cloud backup providers.

How Often:
The frequency depends on several things, such as database size, how busy it is and the criticality of data. There are different types of backup frequency policies that organizations can adapt according to their need.

a) **Weekly:** This type of backup is usually chosen for databases that have only a few transactions every week or contain less important data. A good example can be the payroll database of a very small business company where very little changes are done, and any lost data can be recreated easily.

b) **Daily Once:** This policy is ideal for small companies with more transactions than the company mentioned in the earlier point. Usually, companies that issue manual receipts need this type of backup. As there are manual records, any lost data can be recreated with its help.

c) **Daily Four Times:** This database backup policy is ideal for any database of a mid-sized organizations. These databases go through many changes every day.

d) **Daily Six Times:** This backup policy can be termed as the thorough backup. This policy is for the organizations that will face disastrous consequences or interruption in business functionality if any data loss occurs. Mid-sized retailers and large enterprises usually adopt this policy.

3. Handle passwords securely

What:
Password management is a key part of corporate security, especially when it comes to privileged access management (PAM). Privileged accounts are gems for cyber criminals who attempt to gain access to your sensitive data and the most valuable business information.

The best way to ensure proper security is to use specialized tools, such as password vaults and PAM solutions. This way, you can prevent unauthorized users from accessing privileged accounts and simplify password management for employees at the same time.

How:

- Use one password for one account.
- Use memorable phrases instead of short strings of random characters.
- Use mnemonics or other individual tactics to remember long passwords.
- No sharing credentials with each other, no matter how convenient.
- If MFA is not implemented, require employees to change passwords after a set period.

4. Use multi-factor authentication

What:
As companies move towards tighter controls, passwords may be headed towards obsolescence, changing how people access smartphones, personal computers, websites, and many other password-protected technologies.

Multi-factor authentication (MFA) is a must-have solution for advanced security strategies. Though it's a basic implementation, MFA still belongs among the cybersecurity best practices. It's so effective that the National Cyber Security Alliance has even added MFA to its safety awareness and education campaign.

MFA is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyberattack.

How:
Most MFA authentication methodology is based on one of three types of additional information:

- Things you know (knowledge), such as a password or PIN
- Things you have (possession), such as a badge or smartphone
- Things you are (inherence), such as a biometric like fingerprints or voice recognition

MFA works by requiring additional verification information. One of the most common MFA factors that users encounter are one-time passwords, which are 4–8-digit codes that you often receive via email,

SMS, or some sort of mobile app. With one-time passwords, a new code is generated periodically or each time an authentication request is submitted.

Most modern applications such as Office 365 have MFA built in it. In this case, you need to activate it. Other third applications allow you to set-up MFA on your legacy applications by layering their product on top of your network access.

5. Use the principle of least privilege – Zero-Trust

What:
Having too many privileged users accessing your data is extremely dangerous.

Granting new employees all privileges by default allows them to access sensitive data even if they don't necessarily need to. Such an approach increases the risk of insider threats and allows hackers to get access to sensitive data as soon as any of your employee accounts is compromised.

The principle of least privilege seems similar to the zero trust security model, which is also designed to reduce the risk of insider threats by significantly reducing unwarranted trust.

The zero-trust practice says to grant access only to those users and devices that have already been approved and verified in the system.

How:
Assign each new account the fewest privileges possible and escalate privileges if necessary. And when access to sensitive data is no longer needed, all corresponding privileges should be immediately revoked. Also accounts with admin privileges should only be permitted to conduct administrative actions and should not be able to browse the web or access email.

Specialized Privileged Access Management (PAM) solutions can enforce the principle of least privilege, restricting account creation and permissions to the minimum level a person requires to do a job. Least privilege helps prevent the spread of malware, decreases your cyber-attack surface, improves workforce productivity, and helps demonstrate compliance.

6. Secure third-party access to your data

What:
Remote employees, subcontractors, business partners, suppliers, and vendors – this is only a short list of the people and companies that may access your data remotely.

Third-party access not only entails a higher risk of insider attacks but also opens the way for malware and hackers to enter your system.

A great way to protect your sensitive data from breaches via third-party access is to limit the scope of access that third-party users have and know who exactly connects to your network and why.

Create a sand box environment, that is disconnected from the rest of your network. This sandbox environment will contain the program/data that the third-party will access only.

How:
You can setup a virtual instance that mimics your existing applications on premise, or simply use SaaS environments to setup such an instance.

7. Be wary of phishing and spear-phishing

What:
Phishing emails are sent often to random recipients. These phishing emails usually contain a gift offer or look like an official looking email from a well-known company to track a shipment. Clicking on a link in these emails may download a malware to your computer or direct you to enter your coordinates such as email and password into a form. Information gathered through phishing is normally sold to other cybercriminals who will in turn use a technique called spear-phishing to craft a customized email, or other communication method (SMS or social media) to defraud the victim. An example of spear phishing is when the victim receives an email, purportedly from a CEO, to wire money because the CEO lost their briefcase. Such emails almost always include the term "This is highly confidential" or "do it now" or other forms of written intimidation elements.

How:
- Get a properly configured spam filter and ensure that the most obvious spam is always blocked.
- Educate your employees about popular phishing and spear-phishing techniques and the best ways to deal with them.
- Use Doman Name System (DNS) filtering to block malicious websites and filter out harmful or inappropriate content. This ensures that company data remains secure and allows companies to have control over what their employees can access on company-managed networks.

8. Raise employee awareness

What:
Your employees are the key to protecting your data.

How:
A sure way to deal with negligence and security mistakes by your employees is to educate them on why safety matters:

- Raise awareness about cyber threats your company faces and how they affect the bottom line.
- Explain to your employees the importance of each computer security measure.
- Show examples of real-life security breaches, their consequences, and the difficulty of the recovery process.
- Regularly, test employee awareness by using available on-line, cloud-based platforms.
- Ask employees for feedback regarding the current corporate security system.

Recruit your employees as part of your defenses and you'll see that instances of negligence and mistakes will become less frequent. Training for all users on proper use of the company's equipment and resources

is essential for mitigating security risks and improving awareness. In addition, it optimizes work processes, efficient use of tools, and improves the overall business experience for team members and clients alike.

9. Set-up an incident reporting mechanism

What:
Incident reporting encourages a culture of security and streamlines and helps maintain regulatory compliance.

How:
A Standard Operating Procedure (SOP) for reporting Cybersecurity incidents should be easy to use by all. Complicated forms should be avoided. An escalation process to report to the right people should be clearly identified and finally, the reporting should be auditable to show compliance with regulations and standards.

10. Keep your systems up to date

What:
Updating systems as per manufacturer recommendations minimizes known vulnerabilities. Anti-virus and anti-malware applications must have their databases automatically updated.

Security Patching fixes vulnerabilities on software and applications that are susceptible to cyber-attacks, ensures system uptime, and most importantly, ensures compliance with regulatory bodies [i]that require it. Anti-virus and anti-malware applications databases must be always current

How:
Use Patch Management software to automate the software update on your infrastructure, including firmware on routers and switches. For anti-virus and anti-malware applications, use automatic database update to ensure that you are protected from emerging known threats and their corresponding footprints

Other complementary practices that should be considered:

1. Assign someone (with authority) to oversee cybersecurity across all departments.
2. Add cybersecurity as a line item in your budgeting process.
3. Commit to continual improvement and ongoing awareness training.
4. Consider obtaining a cyber insurance.

Glossary

Adware: Adware, or advertising-supported software, is any software package that automatically renders advertisements to generate revenue for the author. The advertisements may be in the user interface of the software or presented in the web browser. Adware may cause tabs to open automatically that display advertising, make changes to the home page settings in your web browser, offer ad-supported links from search engines, or initiate redirects to advertising websites.

APT: An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by cyber criminals targeting a specific entity. An APT usually targets organizations and/or nations for business or political motives.

Backdoor: A backdoor is a type of trojan that enables threat actors to gain remote access and control over a system. The backdoor is often the final stage in gaining full control over a system.

Botnet: A botnet is a few internet-connected systems infected with malware that communicate and coordinate their actions received from command and control (C&C) servers. The infected systems are referred to as bots. The most typical uses of botnets are DDoS attacks on selected targets and the propagation of spam.

Browser hijacker: A browser hijacker is any malicious code that modifies a web browser's settings without a user's permission, to inject unwanted advertising into the user's browser or redirect to fraudulent or malicious sites. It may replace the existing home page, error page, or search page with its own. It can also redirect web requests to unwanted destinations.

Bulletproof hosting: Bulletproof hosting is a service provided by some domain hosting or web hosting firms that allows their customer considerable leniency in the kinds of material they may upload and distribute. This type of hosting is often used for spamming, phishing, and other illegal cyber activities.

Cryptojacking: Cryptojacking is malicious cryptomining and the covert use of a systems computer resources to mine cryptocurrency. Cryptojacking is initiated by malware or through web cryptominers embedded in website code.

Domain Name System (DNS) Filtering: DNS filtering is the process of using the domain name system to block malicious websites and filter out harmful or inappropriate content. This ensures that company data remains secure and allows companies to have control over what their employees can access on company-managed networks.

Drive-by download: A drive-by download is any download that happens without a person's consent or knowledge.

Dropper: A dropper is a program or malware component that has been designed to "install" some sort of malware (ransomware, backdoor, etc.) to a target system. The dropper may download the malware to the target machine once it is received from the command and- control server or from other remote locations.

Exploit kit: An exploit kit is a software kit designed to run on web servers with the purpose of identifying software vulnerabilities in client machines communicating with it and discovering and exploiting vulnerabilities to upload and execute malicious code on the client.

Fast flux botnet: Fast flux is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies. It can also refer to the combination of peer-to-peer

networking, distributed command and control, web-based load balancing and proxy redirection used to make malware networks more resistant to discovery and countermeasures.

Information stealer: An information stealer is a trojan that can harvest keystrokes, screenshots, network activity, and other information from systems where it is installed. It may also covertly monitor user behavior and harvest personally identifiable information (PII) including names and passwords, chat programs, websites visited, and financial activity. It may also be capable of covertly collecting screenshots, video recordings, or can activate any connected camera or microphone. Collected information may be stored locally and later retrieved or may be transmitted to a command-and-control server.

Loader: A loader is a type of malware or malicious code used in the loading of a second-stage malware payload onto a victim's system. The loader can hide a malware payload inside the actual loader code instead of contacting a remote location to download a second stage payload.

Malvertising: Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages. Malvertising is often used in exploit kit redirection campaigns.
Mobile trojan: A mobile trojan is a trojan designed to target and infect mobile phones running Android, iOS, Windows or other mobile operating systems.

Phishing: A campaign of mass emails that goes after large numbers of email addresses tp gather credentials "en masse"
"Phishing is just kind of generic, low-tech, not targeted attacks," says Aaron Higbee, cofounder and CTO of anti-phishing firm Cofense (previously known as PhishMe). "They don't particularly care about who their target is. They're just casting a wide net trying to snare as many people and as many companies as possible."
Ransomware: Ransomware is computer malware that installs covertly on a victim's computer, encrypts files, and demands a ransom be paid to decrypt the files or to prevent the attacker from publishing the victim's data publicly.

Remote access trojan (RAT): A remote access trojan (RAT) is malware that allows covert surveillance or unauthorized access to a compromised system. RATs make use of specially configured communication protocols. The actions performed vary but follow typical trojan techniques of monitoring user behavior, exfiltrating data, lateral movement, and more.

Rootkit: A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software.

Scareware: Scareware is a form of malicious software or website that uses social engineering to give the perception of a threat to manipulate users into buying or installing unwanted software. Scareware misleads users by using fake alerts to trick them into believing there is malware on their computer and manipulates them into paying money for a fake malware removal tool or allowing an entity remote access to their system to clean the malware. Instead of remediation, the software or remote entity delivers malware to the computer.

Sinkhole: A DNS sinkhole, also known as a sinkhole server, is a DNS server that gives out false information, to prevent the use of the domain names it represents. Traffic is redirected away from its intended target. DNS sinkholes are often used to disrupt botnet command and control servers.

Spam: Spam is an unwanted, unsolicited message that can be received through email or SMS texts. Spam is sent to many users in bulk. It is often sent through the means of a botnet. Spam can contain advertising, scams, or soliciting. In the case of malspam or malicious spam, it contains malicious attachments or links that lead to malware.

Spear phishing: is the act of sending and emails to specific and well-researched targets while purporting to be a trusted sender. The aim is to either infect devices with malware or convince victims to hand over information or money.

Spyware: Spyware gathers information about a person or organization without their knowledge. It may assert control over a computer without the user's knowledge

Trojan: A trojan is malware which is used to compromise a system by misleading users of its true intent. Trojans typically create a backdoor, exfiltrate personal information, and can deliver additional malicious payloads.

Worm: A computer worm is malware that replicates itself in order to spread to other computers. Worms typically spread through the computer network or removable storage devices that are shared between systems, relying on social engineering to deceive people into running it.