Ace Cloud

7 Key Measures Your Accounting Firm

Can Take to Prevent Cyber Attack

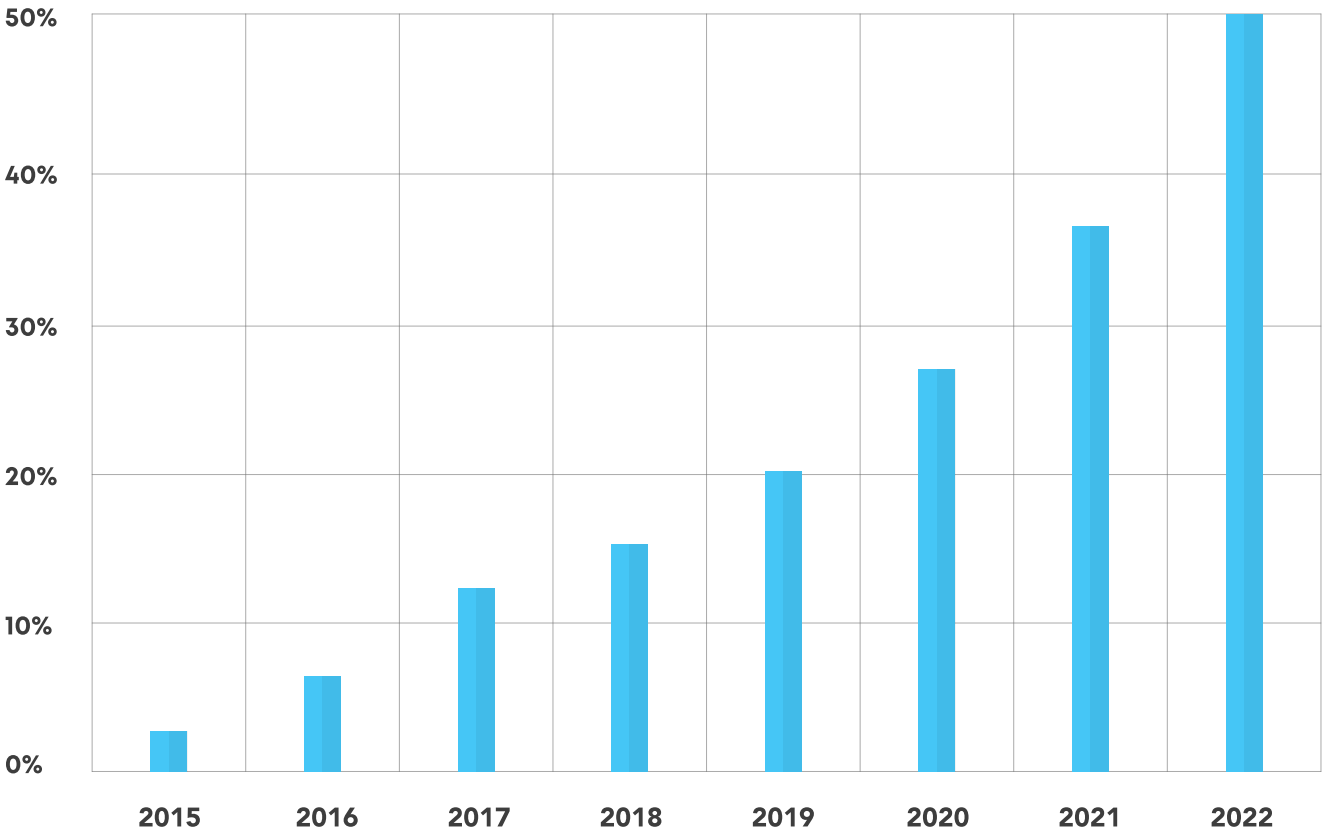
Table of Contents

Introduction: What is a Cyber Attack?

Are you an accounting firm dealing with the collection of sensitive information from both employees and clients? If yes, you must be careful against unwanted attention from hackers and malicious insiders. This is because your employees' and clients' sensitive information might include social security numbers, national ID numbers, addresses, bank details, etc. Access to this information from an unauthorized identity can lead to a cyberattack. It is an unwelcoming attempt to steal data and disable computers or a group of computers in a network. Criminal organizations or cybercriminals devise different strategies to launch a cyberattack that includes ransomware, malware, phishing, or another method. The product used for carrying out a cyberattack is called a cyberweapon.

Cyberattacks can be fatal, ranging from installing spyware on personal computers to destroying the infrastructure of large MNCs.

According to a Report generated by Check Point 2022, cyberattacks against corporate networks increased by 50% in 2021 compared to 2020.



This whitepaper will help you learn some of the most common types of cyberattacks and effective cybersecurity measures by which you can protect your accounting firm from potential cyberattacks.

Types of Cyber Attacks

Cyberattacks come in various forms. If you know them all, it will be easier for you to protect your networks and systems against them. Let's look at some of the most common forms of cyber-attacks that can affect an individual, or a large business, depending on the scale.

Malware:

Cyberattacks come in various forms. If you know them all, it will be easier for you to protect your networks and systems against them. Let's look at some of the most common forms of cyber-attacks that can affect an individual, or a large business, depending on the scale. Using antivirus software, firewalls, updating operating systems, and browsers are some of the most effective ways by which you can prevent a malware attack.

Phishing:

Phishing is amongst the most widespread types of cyberattacks where a perpetrator sends fake emails or fraudulent messages to trick the victim. The motto behind a phishing attack is to get sensitive information or to deploy malicious software on computer systems. Once the victim opens the email or text message and clicks on the malicious link or opens any email attachment, the phishing attackers gain access to sensitive information.

Double-checking the emails, using an anti-phishing toolbar, updating passwords, etc., are some of the most effective measures by which you can prevent a phishing attack.

Denial-of-Service:

A denial-of-service attack is a type of cyberattack where the attacker makes the resources unavailable in a computer or a group of computers on a network. They target computer systems, servers, etc., to flood them with traffic to put a restriction on resources and exhaust bandwidth. To launch this attack, the DoS attackers often use multiple compromised systems.

Some of the most effective ways to prevent a DoS attack are:

Cryptojacking

Cryptojacking is the process of hacking a computer to mine cryptocurrencies. Here, the cryptojacker infects a website or manipulates the victim to click on a malicious link. In some cases, the cryptojackers use online advertisements with JavaScript for this.

To prevent a cryptojacking attack, you must ensure that all your software programs, including the security apps, are up to date. You can also install an ad blocker as ads are the most common source of cryptojacking scripts.

Structured Query Language (SQL) Injection Attack:

An SQL injection is a threat to web security where a perpetrator manipulates a standard SQL query. For an SQL attack, the attacker injects a malicious code into the victim website search box and makes the server reveal vital information. In most cases, the attacker can change or delete this information and cause persistent changes to the application's content or behavior. You can use an Intrusion detection system to detect unauthorized access to a network. Additionally, you can validate the data supplied by the user to keep a check on the input.

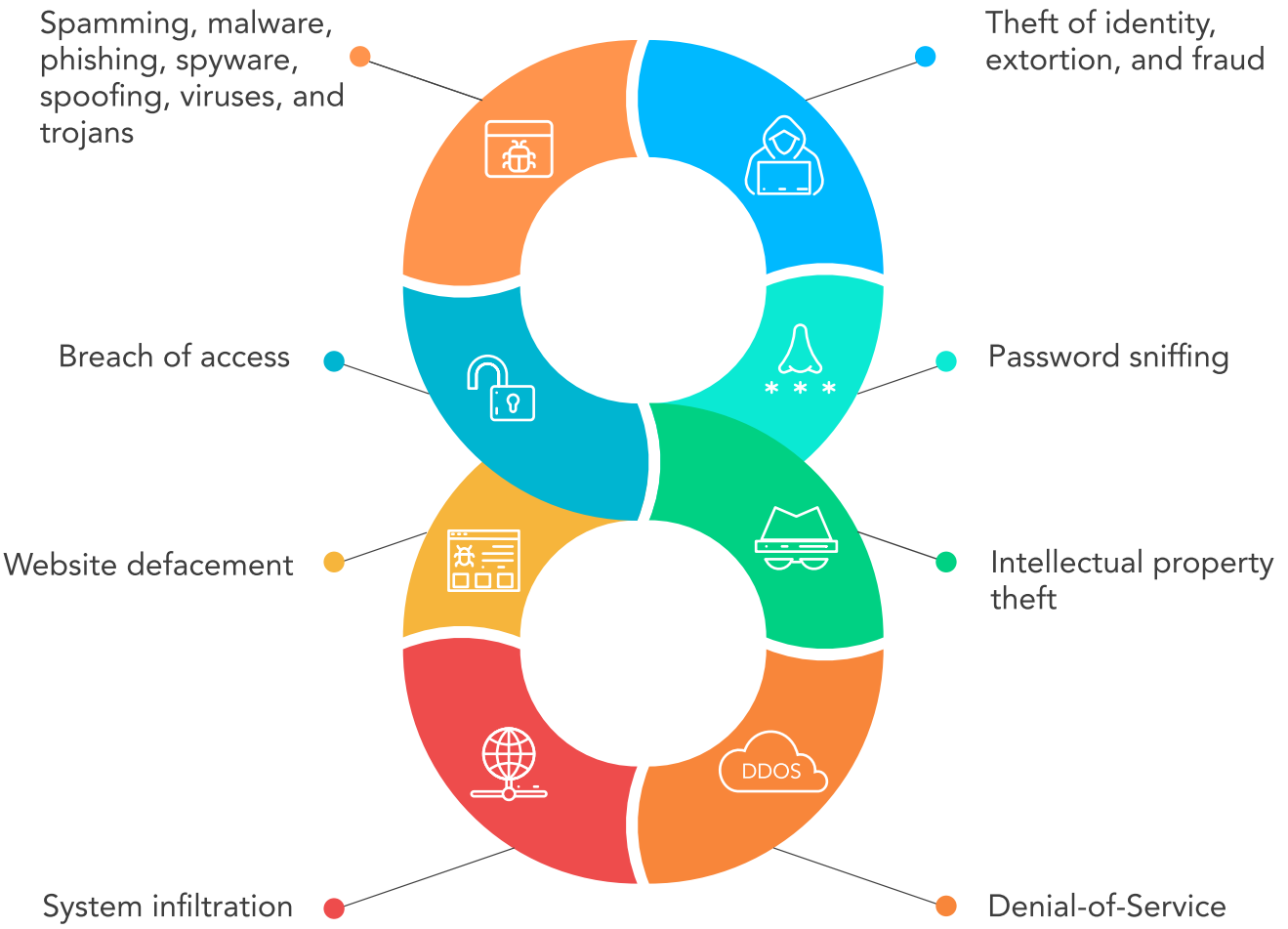
Man-in-the-Middle Attack:

A Man-in-the-Middle Attack, also known as an eavesdropping attack, occurs when an attacker comes in between a two-party transaction. Once the attackers are successful in it, they can hijack the session between a client and host, filtering & stealing vital data. As the attacker's presence during the two-party transaction is unidentified, the victim unknowingly passes all information to the attacker.

Preventing a Man-in-the-Middle attack requires you to be extra cautious of the security of the website you are using. You can encrypt the data on your device & refrain from using Wi-Fi networks open to the public.

Examples of a Cyber Attack

Some of the most common types of cyber-attacks and data breaches include the following:



Know The Varying Nature of Cyber Attacks

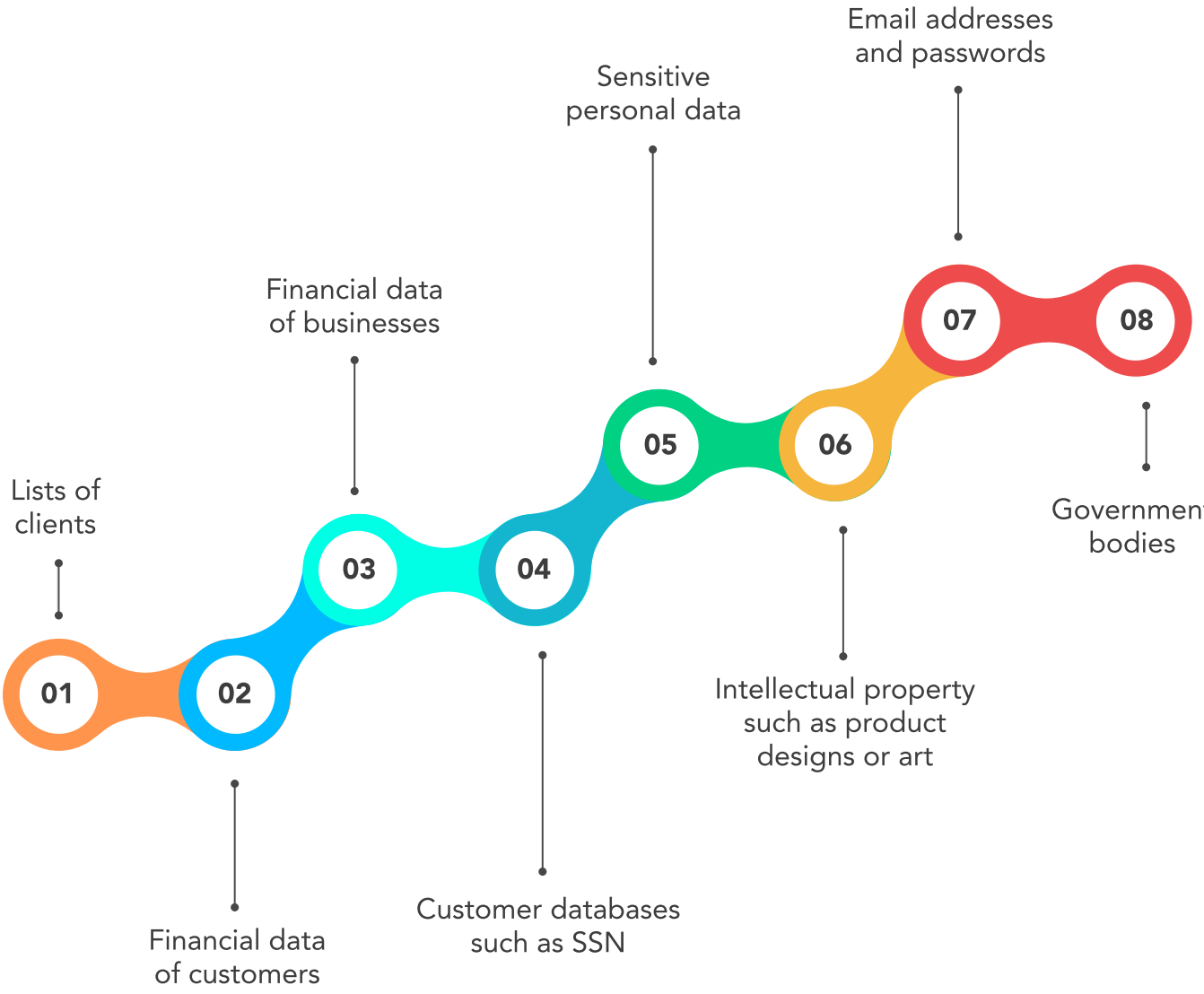
- Accounting industry-based cyberattacks disrupt the accounting workflow of the company. It means that the accounting firm experiences data loss, resulting in business loss.
- Another risk associated with a cyber-attack is data breach when the CPA acts as a perpetrator. Done for the sake of money,

such risks are evoked during the disclosure of the client's financial data by the CPA.

- Lastly, a data breach can also occur when a client's network is infected by a virus, resulting in data exploitation.

Targets of Cyberattackers

While there could be numerous targets of a cyberattacker, the below-mentioned are some of the most common ones:



What Happens During a Cyber Attack?

A cyberattack is an instance when a cybercriminal gets unauthorized access to your data stored on a computer or a group of computers in a network. Ranging from individuals and groups to private organizations and government organizations, cyberattacks can inflict reputational damage to an individual or a business or leak valuable data. A successful cyberattack can damage enterprises, too, causing extensive data loss, downtime, financial loss through ransoms, & more.

- Malware attacks and DoS instances can lead to system and server crashes
- Attackers can alter, delete, insert, or steal data from a system via DNS tunneling and SQL injection
- Attackers can gain entry into a system to steal or damage sensitive information via phishing and zero-day exploit attacks

- Ransomware attacks can make a system defunct until a ransom is paid

The Challenge for Accounting Firms

Usually, small and medium-sized businesses (SMBs) are prone to security-related challenges and are often the prime target of cybercriminals. This is because they tend to pay less attention to information security, controls, and risk assessments. As such, these businesses become more vulnerable as compared to large businesses.

In most cases, SMBs lack sufficient staff in the finance function, and not everyone has the required expertise to identify these problems. Such instances often lead to additional risks. CFOs, CAOs, treasurers, and controllers are especially at higher risk as they can be easily

identified online and because of the frequent online banking transactions they carry out.

Cybercriminals are also aware of the process of accessing bank accounts and the security features of online banking systems.

CPAs and accounting firms performing online banking transactions have at least two risk areas, as mentioned below:

1. The CFO, CAO, treasurer, or the controller often has no clue about corporate account takeovers. As such, they are unaware of the repercussions and liability that may follow.
2. Lack of proper controls over the online banking system.

Even if your accounting firm has fairly stringent controls, persistent cybercriminals' attacks can easily overcome the hurdle. You'd be under the impression that you have a robust security protocol. To mitigate such risks, you can educate your employees and clients about this type of cybercrime. Moreover, the executive finance professional of your organization or the key positions should know the full range of controls and threats associated with the online banking system.

Why is Cybersecurity Important?

Irrespective of the business type, cybersecurity is of epitome importance as it protects your data from damage and the . This includes personal information, sensitive data, intellectual property, information on financial transactions, etc. The lack of a cybersecurity program would not allow you to defend your organization against potential data breaches or cyberattack instances.

- According to Cisco/Cybersecurity Ventures 2022 Cybersecurity Almanac, the cost of cybercrime is predicted to **hit $10.5 trillion by 2025**
- According to a private study, the per-company cost of cybercrime is over $18 million for financial services companies, around 40% higher than the average cost for other sectors

With the rise in the cybercrime rate, neglecting a robust cybersecurity strategy could result in losing sensitive information, money, and reputation.

How Your Accounting Firm Can Prevent Cyber Attacks?

1: Physical Security:

Basics first. Ensure that the physical space with client's information is restricted. You can mandate using the key cards of your employees, visitor logs, badges, and CCTV cameras to ensure that no unauthorized person enters the accounting office.

With the work-from-home culture in place, you must ensure that the work devices employees use at home are also physically secure.

Besides, you can mandate the use of hardware encryption for all work devices to ensure that the data on these devices cannot be retrieved without an encryption key.

2: Store Data on the Cloud:

In a conventional method, all documents are stored in physical files, in the form of hard copies. This often resulted in data theft or damage. While nowadays, computer storage has substituted those hard copies of data, it is still not fully secured and is subject to cyberattacks and data leakages. Businesses often encounter threats and require full-time IT support to mitigate the attacks.

Compared to the computer storage method, data storage in the cloud is secure and cost-effective. With cloud technology, threats can easily be detected and acted upon. Such a solution offers accounting firms an excellent opportunity to safeguard their crucial data from breaches compared to other storage means.

3: Keep a Check on Sensitive Data Transfers:

Monitoring and controlling the transfer of accounts-related information should be of prime importance for your accounting firm. You can use Data Loss Prevention (DLP) solutions to achieve this. The technology used in this solution uses Personal Identifiable Information (PII) and financial information to search for it amongst multiple file types using content inspection and contextual scanning. This way, you can effectively identify and monitor the movement of sensitive files.

In addition to the above, accounting firms can implement specific policies to control the transfer of sensitive data. Whether by messaging

applications, file-sharing applications, or email, DLP solutions can restrict sensitive data transfer over the internet. Besides, they can prevent the upload of sensitive data on the cloud or prohibit copy-pasting the data into email bodies.

4: Encrypt your data:

Data encryption is one of the most effective ways by which you can secure your confidential information. Whether you are transferring data or uploading it online, you must encrypt it first or use a cloud storage service that offers end-to-end data encryption. In case you're using a software program to encrypt your data, ensure that you've kept the decryption key safe, else you will never be able to retrieve the data. You can either go to the Control Panel settings or avail VPN services to ensure that your online data transfers are secure and anonymous.

5: Conduct regular audit of your cyber security policies:

Ensuring smooth working of your cybersecurity protocols is essential. As a good practice, you must regularly check the software, systems, servers, and cloud solutions by reviewing the cybersecurity policies. You can check how the recovery process works for your business by accessing the backed-up files.

Next, check if there are any vulnerabilities or if the backed-up files are corrupt. If any unused software programs are installed on your computer, uninstall them to reduce the risk of cybercriminals manipulating the software to steal or damage your confidential data. Additionally, ensure that all the devices are protected with passwords so that your data can remain secure whenever any of the devices are lost or stolen.

6: Educate your employees:

Cybercrimes like phishing attacks can target your employees directly. Attackers can steal login credentials or deploy malicious software in a company network by making your employees click on a malicious link or downloading an attachment. Most ransomware attacks are carried out via phishing.

Although solutions like Trusted Platform Module capabilities, antimalware, and Zero Trust architecture can reduce the risk of phishing attacks or causing excessive damage, training your employees can be equally effective in mitigating a threat. By training your employees on how to detect a cyber threat and what steps to take in case they are targeted, you can raise awareness of phishing attacks and enable your employees to combat them whenever required.

7: Secure Flash Drives:

While using a flash drive serves the purpose of data storage, when it is lost or stolen, all your sensitive data can be at risk. If your employees use flash drives or external hard drives and take them out of your company premises, any of your company data could be at high risk, especially when they are lost or stolen.

This is where you can use Data Loss Prevention (DLP) tools. Most DLP tools offer device control features that allow you to block the use of peripheral and USB ports. In some cases, you can use a DLP tool to limit the use of the flash drive and ensure its usage for trusted company-issues devices only.

Conclusion

CPAs and accounting firms have access to valuable client data, and preventing a cyberattack is vital for the survival of your business. If you are one of them, you must be very careful to protect those data. Physical security, storing data on the cloud, encrypting data, performing regular audits of your cyber security policies, etc., are some of the most effective ways to prevent cyber-attacks. However, educating your employees about cybercrimes and how to deal with them can go a long way in reducing risks caused by human error.

By leveraging the aforementioned best practices, you can seek a safe and secure environment for your organization's valuable asset, i.e., data.