A cyber attack is a kind of attack that targets a computer or a computer network in an attempt to destroy, steal, or alter any information present in it. The attacker can be a person or a process that gained unauthorized access or use. There are several types of cyber attacks: Denial-of-service [DoS] and distributed denial-of-service [DDoS] attacks, Man-in-the-middle [MitM] attack, Phishing attacks, Drive-by-download attack, Password attack, SQL injection attack, Cross-site-scrpting [XSS] attack, Eavesdropping attack, Birthday attack, Malware attack

How cyber attacks have evolved in recent years?

Cyber attacks went through a great change over decades, using new techniques and methods, while maintaining their main goal is remaining the same. In the beginning cyber attacks were simple and not very developed, but as the Internet grew, threats became more complex while cyber attackers are gaining notoriety rather than financial and informational gain. By the 2000s, cyber attacks transformed into a profitable business model introducing ransomware and spyware designed to extract financial information. They started using sophisticated tools and tactics to conduct espionage and disorder services. In our days, cyber attacks are more sophisticated, involving developed phishing techniques and other methods.

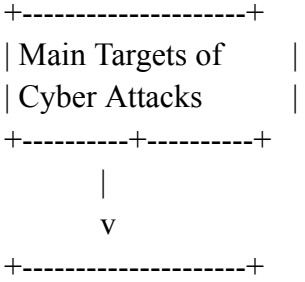
Sometimes the most dangerous ways to harm us are invisible and untouchable, this is the case with cyber attacks which are showing themselves only to defeat us.

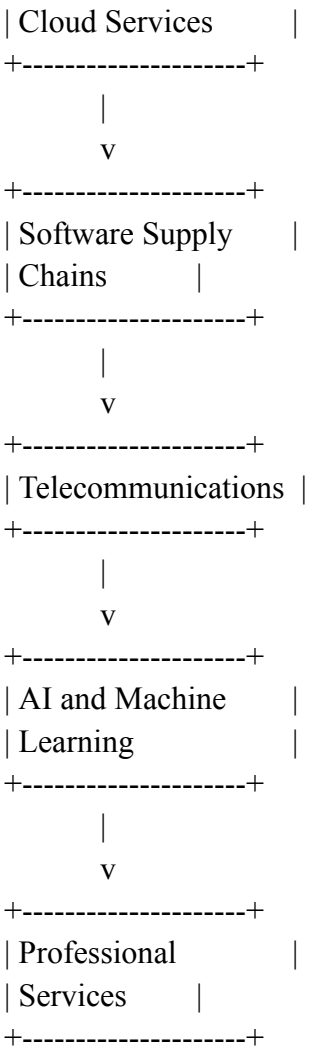
> “Cybercrime is the greatest threat to every company in the world.”
>
> — Ginni Rometty, Former CEO of IBM

What Industries Are the Most Impacted by Cyber Attacks

In 2024, several tech industries were significantly influenced by cyberattacks. There are 5 most affected industries by cyber attacks:

- Cloud services
- Software supply chains
- Telecommunications
- AI and machine learning
- Professional services





Cloud Services

Cloud Services are affected by cyber attacks due to some factors which include: Rich data environment, scalability and complexity, shared responsibility method, remote access and rapid adoption. According to Statista in 2023, the share of cloud cyberattacks reached 16.6% which is higher than in 2022 which was 13.2%. One example of a Cloud Services cyber attack from 2023 is the MOVEit hack

Cloud cyber attack targets cloud-based service platforms, such as storage and computing services or hosted applications as a service (PaaS) or software as a service (SaaS) model.

Specific types of cyber attacks that affect the industry

Here are several types of cyber attacks that affect the industry of cloud services:

- **Denial-of-Service attacks**, is a type of cyber attack that aims to make a network or computer unavailable for the user. Denial-of-Service attacks involve spamming a cloud service with a large amount of traffic or spam, which can make the network

overwhelmed or overworked and make it unable to process legitimate requests. Cloud-based DoS attacks can be particularly challenging to defend against, as the scale and complexity of cloud environments can make it difficult to identify and reduce the attack.

- **Account Hijacking**, Cloud account hijacking is a process in which an user or organization's cloud account is stolen or hijacked by a hacker. Cloud account hijacking is a common method in identity theft schemes in which the hacker uses the stolen account information to conduct degrading or unauthorized activity. When cloud account hijacking occurs, an attacker typically uses a compromised email account or other credentials to impersonate the account owner
- **Security Misconfiguration** refers to the failure of cloud computing resources and infrastructure to protect and prevent against cyber attacks. This type of attack can include failure to properly set access controls, failure to properly configure and secure systems and applications, and failure to regularly update and patch systems and applications.

The consequences of cloud cyber attacks

Cloud attacks can have grave consequences, such as data breaches, data loss, unauthorized access to sensitive information, and disruption of services.

Case study of cyber attacks in the Cloud Service industry

Kaseya

In July 2021, IT solution provider Kaseya experienced an attack on its remote monitoring and network perimeter security tools. It was a supply chain ransomware attack, designed to gain administrative control over Kaseya services and use them to infect the networks of managed service providers and their customers.

How can Cloud services respond effectively to cyber-attacks?

- Implementing access controls
- Encrypting data

- Implementing backup
- Recovery processes
- Regularly updating
- Patching systems and applications.

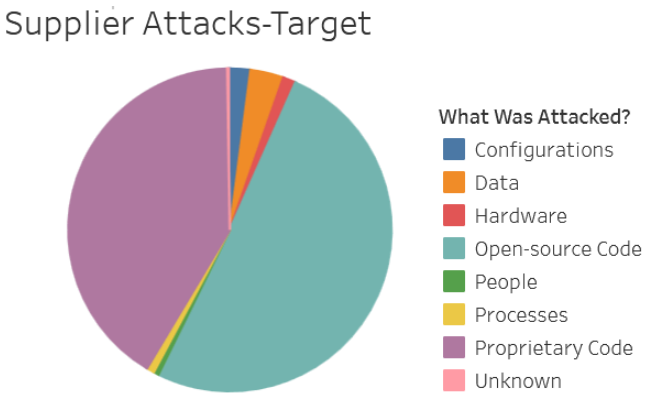
Software Supply Chains

The Software Supply Chains industry has become one of the main targets for cyber attackers because of its role in software development and distribution. The number of Software Supply Chains cyber attacks is growing every day. "There has been an astonishing 742% average annual increase in software supply chain attacks over the past 3 years". One example of Software Supply Chains cyber attack is Okta (October 2023).

Specific types of cyber attacks that affect the industry

A software supply chain attack occurs when a hacker gets unauthorized access and makes a different software in the complex software development supply chain to compromise a target below on the chain by putting their own malicious code. These inserts can be used to further destruct code by obtaining system access or to directly deliver a malicious payload. Recently created software products contain a large number of dependencies on other code, so finding out which vulnerabilities compromise which products is a solvable organizational and technical feat.

- **Stolen certificates**, if an attacker steals a certificate used to vouch for the legitimacy or safety of a company's product, they can peddle malicious code under the guise of that company's certificate.
- **Compromised software development tools or infrastructure**, hackers are using tools for building software applications to introduce security weaknesses in the development process—even before the process is used to create an application.
- **Malware preinstalled on devices** when cyber attackers put malware on phones, Universal Serial Bus (USB) drives, cameras, and other mobile devices, and when the user connects it to their system or network, virus code gets introduced.



The consequences of Software supply chains cyber attacks

For numerous cyber attackers, their main goal is to gain financial and personal data for their personal use. Software supply chains enclose various businesses, all varying in size, and to a proficient cyber attacker, targeting a smaller entity with less powerful security measures and limited resources for software maintenance is merely an initial move. Stolen credentials can serve as a way to more substantial targets possessing larger data possibilities further up the supply chain.

Case study of cyber attacks in the Cloud Service industry

SolarWinds

SolarWinds was the cyber attack that put software supply chain attacks on the map. Its IT monitoring system named Orion, which is used by over 30,000 organizations including federal, state, and local agencies, was compromised by cyber attackers. This enabled the hackers to deliver backdoor malware in an Orion software update.

Not only could the hackers access and imitate the user' accounts, the malware could also access system files and work among SolarWinds' legitimate activities, going undetected even by antivirus software.

How can the Software supply chains industry respond effectively to cyber-attacks?

- Audit unapproved shadow IT infrastructure
- Have an updated and powerful software asset inventory in place
- Assess a vendor's security posture
- Treat validation of supplier risk as an ongoing
- Use client-side protection tools

Telecommunications

The Telecommunication sector is a high value sector for cyber attacks, because its high reliance on telecom networks for everything including voice calls and financial transactions made the Telecommunication industry a perfect target for Distributed denial-of-service [DDoS] attacks. This type of cyber attack can bring a malicious impact on telecom networks, causing service outages, degrading networking performances, and leading to financial and reputational damage.

Specific types of cyber attacks that affect the industry

- **Denial-of-service [DoS] and distributed denial-of-service [DDoS] attacks** is a system that denies the system resources so that it can't answer to the service request, in this kind of cyber attack , the network or machine resources are made unavailable for the user by interrupting the service of the host which is connected to internet. DDoS attacks are particularly common in the telecom sector due to the interconnected nature of their networks.
- **Insider threats**, these are one of the major risks for this industry, cyber attacks have increased in recent years because of more remote job models and connections to unsecured networks. Phishing is one of the main concerns where attackers send malicious links through emails or messages.

- **Supply chain risks,** as the telecommunication industry deals with third-party entities such as vendors, data managing services, and managed service providers. If cyber security is weak it can give cyber attackers an opportunity to hack telecom networks. All that is needed is a weak link in the supply chain to cause severe damage.

  The consequences of Telecommunication industry cyber attacks
  - Data breaches
  - Operational disruption
  - Financial losses

  Case study of cyber attacks in the Telecommunication industry

Vermilion Strike

It is a threat that affects Linux and Windows systems, and the telecommunication industry is very sensitive to it. The Linux malware is completely undetected by vendors and the damage assures remote access to the cyber attackers to upload files, write to files and run shell scripts. Vermilion Strike is not used in mass attacks, in contrary is used in targeted attacks.

How can the Telecommunications industry respond effectively to cyber-attacks?

- Securing data and communication systems
- Encryption techniques
- Regular update

AI and Machine Learning

Because of its fast growth, infiltration in our society and enormous amounts of data and information being used, the AI and machine learning industry became one of the main targets for cyber attacks. Hackers are using vulnerabilities in AI systems in their malicious goals. AI systems can malfunction when exposed to untrustworthy data, information and hackers are exploiting this issue in their personal achievements.

Specific types of cyber attacks that affect the industry

- **Evasion attacks** occur after an AI system is deployed, attempting to alter an input to change how the system responds to it.
- **Privacy attacks** occur during deployment about the AI or the data it was trained on in order to misuse it.
- **Abuse attacks,** this attack involves the insertion of incorrect information into a source, such as a web page or online document, that an AI absorbs.

The consequences of Professional services cyber attacks

- Data breaches

- Loss of intellectual property
- financial losses

How can the AI and machine learning industry respond effectively to cyber-attacks?

- An intrusion detection system (IDS)
- Signature-based detection
- Anomaly-based detection
- A hybrid detection approach

Professional Services

Among all Professional services, the legal sector stands out as one of the major focuses for cyber attackers. Legal organizations often manage highly sensitive client information, such as details related to ongoing criminal cases or corporate mergers and acquisitions. This data can be of major value for criminals aiming to exploit insider trading opportunities, gain competitive advantages in negotiations, or even manipulate the course of justice, or for financial resources.

Specific types of cyber attacks that affect the industry

- **Phishing** is a type of cyber attack that has a goal to trick users into providing valuable, sensitive information or data via fraudulent emails, website links or SMS. Professional services firms which are storing and using client data are one the main targets for phishing attacks.
- **Ransomware/Malware:** Professional services and legal entities have experienced significant damage from ransomware attacks. This is happening because professional services firms and legal companies are often seen as prime targets for ransomware attacks due to their perceived financial resources compared to businesses in other services. This is likely because professional services firms and legal companies are often seen as prime targets for ransomware attacks due to their perceived financial resources.
- **Supply chain risks,** Cyber attackers are increasingly targeting trusted third-party vendors used by professional services and legal firms. Since these Personal Services firms often act as third parties themselves and depend on numerous external software, consultants, and contractors, it creates numerous potential entry points for attackers.

The consequences of Professional services cyber attacks

- Financial losses
- Reputational damage
- Operational disruptions

Case study of cyber attacks in the Professional Services industry

City law firm

A stark illustration of the risks involved occurred in 2021 when a city law firm, Gateley, fell target to a cyber-attack, resulting in a loss of client data. The market reacted swiftly, causing a nearly 8% drop in share value within an hour of the incident being reported.

.

How can Professional services respond effectively to cyber-attacks?

- Remote Working Data Protection
- Implementation of Firewalls & Network Redundancies
- Utilisation of Corporate VPN's
- Prioritising Data Backups
- Regular Updates of Software & Systems

Explore more cybersecurity providers on TechBehemoths.

The impact of COVID-19 on cyber attacks

The COVID-19 pandemic had a paramount impact on a billion people's lives, making everyone of us change their everyday routine and separate their lives to before and after. But it also brings a change in cyber attacks by bringing some circumstances that also affect our society.

A crucial factor in the growth of cyber attacks during the pandemic is the possibility of working remotely from home. Since the beginning of the pandemic, there has been an increased number of cyber attacks, for example 600% increase in phishing attacks in March 2020.

„The World Economic Forum (WEF) reported that the pandemic led to a 50.1% increase in cyber-attacks and an associated 30,000 cyber-attacks which were specifically COVID-19 related”. Also, it is said that Google blocked 18 million malware and virus-related emails. Being isolated made people spend more time online, also another factor is that some people who remained unemployed because of the pandemic may have used cyber crimes to support themselves during these hard times.

Considering all these factors it is clearly shown that hackers and cyber attackers were working and using billions of people's hard times, problems, worries, and anxiety making them more vulnerable to their attacks.

Conclusion

Fast-growing digitalization has made us more dependent on technologies that can bring us much useful information and make our lives easier and on the contrary, can bring us harm and danger if not used correctly.

Everyone can be its victim from a university student to a big company or whole industry. As we discussed earlier there are different types of cyber attacks but all are different and use various methods but all of them have a common goal, which is to gain access to information and use it for malicious motives.

Cloud services, Software supply chains, Telecommunications, AI and machine learning and Professional services are some of the most affected industries by cyber-attacks. It is important to mention that all of us and all these industries can prevent and make a defense against hackers and cyber attackers by protecting data access and information and making regular updates and checkups to make sure that their protection is working.

In conclusion, all of us should be careful and think about protection against cyber attacks and stay up to date with the latest security best practices to not risk our data and information.