# Cyberattacks in 2022-2024 reveal growing digital vulnerabilities and costs



In recent years, the world has witnessed a series of devastating cyberattacks that have profoundly impacted organisations, governments, and millions of individuals globally. These incidents not only exposed vulnerabilities within digital infrastructures but also underscored the growing sophistication and scale of cybercrime. In 2024, cybercrime costs were estimated to have surpassed a staggering $9.5 trillion, positioning the shadow economy of cybercrime as the third-largest in the world, after the United States and China.

Among the most significant cyberattacks in recent history, a number stand out for their scale, method, and repercussions.

In 2022, Uber experienced a high-profile breach when a teenager linked to the Lapsus$ hacking group employed a tactic known as multi-factor authentication (MFA) fatigue to gain internal access. By repeatedly sending login requests, the attacker eventually tricked an employee into approving access, which led to unauthorised control over internal systems including Slack, financial dashboards, and source code repositories. This incident highlighted weaknesses in enterprise identity security, particularly in the absence of behavioural monitoring and zero-trust policies. Fortunately, no user data was compromised.

That same year, Australian health insurer Medibank suffered a severe breach resulting in the theft of medical and personal records of approximately 9.7 million customers, representing nearly 40% of Australia’s population. The attackers accessed sensitive treatment information, mental health notes, and personal identifiers through stolen credentials and demanded a ransom, which Medibank declined to pay. The breach sparked public outrage, prompted government cybersecurity reforms, and led to a significant drop in the company’s stock price.

Also in 2022, LastPass fell victim to a breach involving the compromise of a developer’s home computer. Attackers exploited these credentials to exfiltrate encrypted password vault backups from a third-party cloud provider. While the vaults remained encrypted, the theft of metadata including URLs and customer email addresses severely damaged user trust and served as a cautionary tale about the vulnerabilities linked to cloud storage and identity management.

In 2023, the MOVEit Transfer software was exploited through a previously unknown zero-day vulnerability by the Clop ransomware group. This attack affected over 2,500 organisations worldwide, ranging from government contractors to universities and financial institutions. The incident triggered a wave of concern regarding software supply chain security and the imperative of robust vulnerability management.

Genetic testing company 23andMe experienced a credential stuffing attack in 2023, where attackers utilised reused passwords obtained from previous breaches to access approximately 14,000 accounts. Due to 23andMe’s relative-matching features, genetic data from roughly 6.9 million individuals was accessible, raising alarms about the potential misuse of genetic information and triggering legal actions.

Telecommunications giant T-Mobile confirmed in early 2023 that misconfigured application programming interfaces (APIs) led to the exposure of personal data belonging to around 37 million users. While financial details were not compromised, the breach represented the company’s eighth since 2018, drawing regulatory scrutiny and questions about improvements in security measures.

In March 2023, Capita, a major UK outsourcing firm providing public services, was hit by a ransomware attack by the Black Basta group. The incident caused widespread disruption to government services including military recruitment, national pension systems, and housing benefits. The breach exposed internal emails and insurance records, estimated to cost over £20 million in recovery efforts and prompted reviews of cybersecurity protocols for public sector vendors.

Western Digital, in the same month, faced a cyberattack that led to the theft of approximately 10 terabytes of internal data and the temporary shutdown of MyCloud services. This attack caused significant inconvenience for customers reliant on cloud storage for business and personal use.

Early 2024 saw Change Healthcare, a central processor for insurance claims and prescription benefits in the United States, crippled by a ransomware attack attributed to the BlackCat/ALPHV group. The incident resulted in a $22 million ransom payment and caused widespread paralysis of prescription systems, delaying medication access and impacting hospital revenue cycles nationwide.

Microsoft disclosed in 2024 that Russian state-linked hackers, identified as the Midnight Blizzard group (also known as APT29 or Cozy Bear), breached executive email accounts using a combination of password spray attacks and OAuth permission exploits. The espionage operation went undetected for months, involving senior executives and cybersecurity personnel. This attack prompted thorough security reviews and revisions of internal access controls.

Additionally, pharmaceutical distributor Cencora reported a cybersecurity incident in early 2024 involving unauthorised access to company data. Although details remain under investigation, the breach raised concerns about potential disruptions to the pharmaceutical supply chain, clinical trial integrity, and compliance under regulatory frameworks like HIPAA and FDA guidelines.

Cyber incidents stretching further back include historic events such as Sony’s 2011 PlayStation Network breach that exposed 77 million accounts, the 2012 Shamoon malware attack against Saudi Aramco which disabled thousands of workstations, and the 2017 WannaCry ransomware outbreak that affected hundreds of thousands of systems globally. These attacks have shaped the evolution of cybersecurity strategies, underscoring the necessity of layered defences, adaptive authentications, rigorous patching, and continuous employee training.

A comprehensive approach to mitigating cyber risks involves practices such as enabling adaptive multi-factor authentication on all accounts, limiting and auditing administrative access, blocking reused passwords, securing APIs and cloud configurations, conducting regular backups with tested restorations, and performing routine phishing tests and incident response rehearsals.

Each of these cyber breaches, whether driven by organised crime, espionage, or opportunistic attackers, reflects the complex interplay between technology, human factors, and evolving threat landscapes. They reveal no system is impervious, and sectors across industries remain vulnerable, continually prompting advancements in cybersecurity resilience and policy.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024> - Supports the claim that cybercrime costs were estimated to have surpassed $9.5 trillion in 2024, making it the third-largest 'shadow economy' globally after the US and China.
* <https://www.cnet.com/tech/services-and-software/uber-hacked-in-multi-factor-fatigue-attack-by-lapsus-group-teen/> - Details the 2022 Uber breach involving MFA fatigue tactics by a Lapsus$ group-linked teenager, confirming the attack methods and impact described.
* <https://www.bbc.com/news/world-australia-62907301> - Confirms the 2022 Medibank data breach that exposed sensitive medical and personal records of approximately 9.7 million Australians and the refusal to pay ransom.
* <https://krebsonsecurity.com/2022/12/lastpass-breach-compromises-customer-vault-backups/> - Corroborates the 2022 LastPass breach where attackers used compromised developer credentials to exfiltrate encrypted password vault backups and related metadata.
* <https://www.zdnet.com/article/moveit-hack-zero-day-exploit-used-by-clop-ransomware-group/> - Confirms the 2023 MOVEit Transfer zero-day exploited by the Clop group affecting over 2,500 organizations worldwide.
* <https://www.nbcnews.com/tech/security/t-mobile-data-breach-exposes-personal-info-37-million-users-rcna72101> - Supports the 2023 T-Mobile breach due to misconfigured APIs exposing data of around 37 million users and the context of it being the company's eighth breach since 2018.
* <https://news.google.com/rss/articles/CBMiY0FVX3lxTFBhTlF0dzVaUlZ0eXd2a01lMndYNE8zcGJSWnVnYm16ZXJqOWJZaVFSQ1ZRMk1TQ0ZnSkxBY1kyclBIeVB3eTU3bnhyYXdnX2p0Wk1jdXRkSnJBM2xyeFo5WDc1RQ?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data