

Biggest Cyber Security Challenges

As companies deploy new IT solutions and technologies, they introduce new security risks. Cybercrime is growing increasingly professionalized, resulting in more numerous, subtle, and sophisticated threats. Cyber threat actors are constantly working to design, build, and evolve solutions to bypass or overcome the most advanced cybersecurity solutions.

All of these factors combine to create a cyber threat landscape in which companies face more significant cyber threats than ever before. In 2022, cyberattacks rose 38% over the previous year. As cyber threat actors refine their techniques, attacks will grow even more common, and companies will face novel and more dangerous cyber threats.

While some cyber threats stand the test of time, many others ebb and flow from year to year. In this era, these are some of the most significant cybersecurity challenges that businesses should prepare to face.

Ransomware Extortion



Ransomware began as malware focused on extorting payments via data encryption. By denying legitimate users access to their data by encrypting it, the attackers could demand a ransom for its recovery.

However, the growth of ransomware threats has resulted in focused security research designed to identify and remediate these threats. The process of encrypting every file on a target system is time-consuming — making it possible to save some data by terminating the malware before data is encrypted — and companies have the potential to restore from backups without paying the ransom.

Double extortion attacks added data theft to data encryption, and some ransomware operators have shifted to focus solely on the extortion effort, skipping encryption entirely. These ransomware data breaches are faster to carry out, harder to detect, and cannot

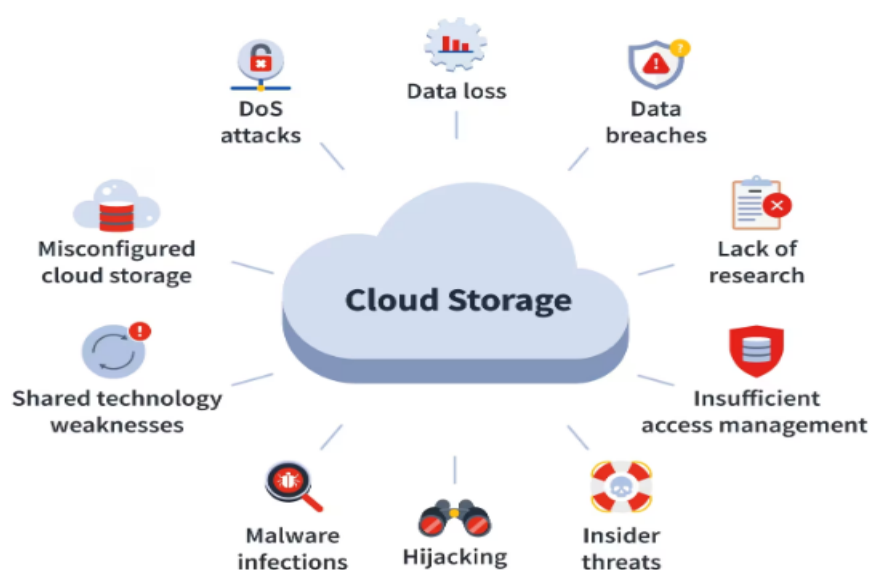
be fixed using backups, making them a more effective approach for cybercriminals and a greater threat to businesses.

Cloud Third-Party Threats

Companies are increasingly adopting cloud computing, a move with significant security implications. Unfamiliarity with cloud security best practices, the cloud shared security model, and other factors can make cloud environments more vulnerable to attack than on-prem infrastructure.

While cybercriminals are increasingly targeting cloud infrastructure with exploits for new vulnerabilities, an emerging and worrying tactic is the targeting of cloud service providers. By targeting cloud service providers and cloud solutions with their attacks, a cybercriminal can gain access to their customers' sensitive data and potentially their IT infrastructure. By exploiting these trust relationships between organizations and their service providers, attackers can dramatically increase the scale and impact of their attacks.

Cloud Security Risks You Need To Know



Mobile Malware



As mobile devices have become more widely used, mobile malware has emerged as a growing threat. Mobile malware masquerading as legitimate and harmless applications — such as QR code readers, flashlights, and games — have grown more common on official and unofficial app stores.

These attempts to infect users' mobile devices have expanded from fake apps to cracked and custom versions of legitimate apps. Cybercriminals are offering unofficial versions of apps as malicious APKs via direct downloads and third-party app stores. These apps are designed to take advantage of name recognition to slip malware onto mobile devices.

Wipers and Destructive Malware

While ransomware and data breaches are some of the most visible threats to corporate data security, wipers and other destructive malware can have even greater business impacts. Instead of breaching information or demanding a ransom for its return, wipers delete the data entirely.



While wipers have been relatively rare in the past, they experienced a resurgence in 2022. Multiple families of wipers have been developed and deployed against Ukraine as part of its conflict with Russia. Other countries, including Iran and Albania, have also been targeted by destructive cyberattacks, indicating its growing popularity as a tool for hacktivism and cyberwarfare.

Weaponization of Legitimate Tools

The line between legitimate penetration testing and system administration tools and malware can be a fine one. Often, functionality that cyber threat actors would build into their malware is also built into their targets' operating systems or available via legitimate tools that are unlikely to be recognized as malware by signature-based detection tools.

Cyber threat actors have been increasingly taking advantage of this to “live off the land” in their attacks. By leveraging built-in features and legitimate tools, they decrease their probability of detection and improve the likelihood of a successful attack. Also, the use of existing solutions can help to scale attack campaigns and allow cybercriminals to use the state of the art in hacking tools.

Zero-Day Vulnerabilities in Supply Chains

Zero-day vulnerabilities pose a significant but transient risk to corporate cybersecurity. A vulnerability is a zero day when it has been discovered but no fix is available for the issue. During the window between the initial exploitation of a vulnerability and the vendor's release of a patch for it, cybercriminals can exploit the vulnerability unchecked. However, even after a patch is available, it is not always promptly applied by organizations. Some cyberattack campaigns target vulnerabilities that have been known and “fixed” for months or years. Various reasons exist for these delays, including resource availability, security visibility, and prioritization.

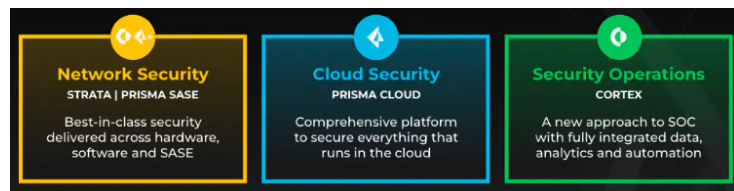
One area where zero-day attacks and unpatched vulnerabilities are especially concerning is the software supply chain. Often, companies lack full visibility into the third-party, open-source code that their applications use. If these external libraries contain unpatched vulnerabilities, cybercriminals can leverage them to attack the organization.

Additionally, widely-used vulnerable libraries create potential attack vectors against multiple organizations.

Global Attacks on Business

Cybercrime is a problem that is rapidly growing on a global scale. In Quarter 3 2022, global cyberattacks increased by 28% compared to the same quarter in 2021. Going into 2023, this trend is only likely to continue. A mature corporate cybersecurity program needs to be capable of defending against threats originating from all around the world. This includes comprehensive threat protection, round-the-clock monitoring, and access to up-to-date threat intelligence.

Security Consolidation



Cybersecurity is growing increasingly complex as IT infrastructures expand and cyber threat actors develop and deploy new attack techniques. As a result, companies need an expanding suite of security capabilities to protect themselves against advanced attacks.

However, attempting to implement these capabilities via standalone, specialized solutions can actually harm corporate cybersecurity by making it more difficult to monitor, configure, and operate an organization's security infrastructure. Security consolidation — in which an organization deploys a single security platform with all of the required security capabilities — improves the efficiency and effectiveness of the organization's security architecture, enhancing its threat management capabilities.

Prevention-Focused Security

Many corporate cybersecurity strategies are detection-focused. Once an active threat has been identified, the organization's security solutions and personnel take action to



mitigate or remediate the ongoing attack. However, a responsive approach to security means that the attacker has a window between launching their attack and its eventual remediation to take malicious actions. During this window, the cyber threat actor can cause harm to the organization and expand and entrench their foothold, making remediation more difficult and expensive.

Instead of focusing on detection, security should have a prevention focus. By identifying and blocking inbound attacks before they reach an organization's systems, a company eliminates the potential threat, damage, and cost to the organization.




Comprehensive Protection

The evolution of corporate IT architectures has provided cybercriminals with numerous potential avenues of attack against an organization. Cloud adoption, remote work, mobile devices, and the Internet of Things (IoT) are only a few examples of new technologies that have introduced new security risks.

Cyber threat actors can identify and exploit a wide range of vulnerabilities to gain access to corporate systems. An effective cybersecurity program is one that provides comprehensive coverage and protection for all potential attack vectors.

Credits: <https://www.checkpoint.com/>

Compiled by: Nonhlanhla Majola

Signature: 

Approved by: Khayelihle Buthelezi

Signature: 