KEEPER®

The Future of Defense

IT Leaders Brace for Unprecedented Cyber Threats

March 2024

Cyber attacks are more sophisticated than ever and IT leaders feel ill-equipped to handle emerging threats

A global survey of more than 800 IT and security executives conducted in 2024 by Keeper Security in partnership with TrendCandy Research, reveals that cyber attacks are increasing in sophistication with novel Artificial Intelligence (AI) threats and advanced, emerging attack techniques. While contending with these new threats, IT leaders are also managing an increased volume of attacks, as 92% of survey respondents report cyber attacks are more frequent today than one year ago. In 2024, security is proving to be increasingly complex with higher stakes than ever.

Keeper Security, the leading provider of zero-trust and zero-knowledge cybersecurity software protecting passwords, passkeys, privileged access, secrets and remote connections, wanted to map the cybersecurity landscape in 2024. Keeper commissioned an independent research agency to gain insights from security leaders around the globe about cybersecurity trends and the future of defence.

Cyber attacks are more frequent and increasingly sophisticated

With rapidly evolving threats, new regulations, advancements such as passkeys and a proliferation of devices – from desktops to spatial computing headsets – cybersecurity is more critical than ever before. An overwhelming 92% of IT and security leaders say that cybersecurity is their number one priority.

These leaders cannot afford to lose focus, as 92% of respondents also reveal that they've seen an increase in cyber attacks year-over-year. Cybercriminals are creative and relentless in their mission to break historically secure solutions and inflict maximum damage on vulnerable organisations.

As the volume of cyber attacks increases, so too does the impact: in fact, 73% of respondents have experienced a cyber attack that resulted in monetary loss. Direct financial impact is one of many consequences of a successful cyber attack, along with business disruption, enduring revenue loss, customer and partner attrition, and tarnished reputation.

IT leaders identify which parts of their organisation have faced attacks

KEEPER

As cybersecurity incidents become more frequent and costly, 95% of IT leaders disclosed that cyber attacks are also more sophisticated than ever – and they are unprepared for this new wave of threat vectors.

95%

of IT leaders say cyber attacks are more sophisticated than ever before

According to respondents, the most serious emerging types of attacks include

1. AI-Powered Attacks
2. Deepfake Technology
3. Supply Chain Attacks
4. Cloud Jacking
5. IoT Attacks
6. 5G Network Exploits
7. Fileless Attacks

KEEPER

Attack vectors IT leaders feel ill-equipped to defeat

- 35% AI-Powered Attacks
- 30% Deepfake Technology
- 29% 5G Network Exploits
- 25% Cloud Jacking
- 23% Fileless Attacks

AI-powered attacks are seen as the most serious emerging threat vector as well as the most challenging to handle. Malicious actors weaponise AI to speed up and scale common attack techniques such as phishing and password cracking. This spotlights the need for a proactive approach to cybersecurity – one that combines advanced defence mechanisms and basic best practices to mitigate and fight evolving threats.

Globally, IT leaders plan to increase their overall AI security through

Data Encryption
51%

Employee Training and Awareness
45%

Advanced Threat Detection Systems
41%

As cyber threats continue to worsen and evolve, IT leaders must adapt their tactics and strategies, using a multi-layered approach to security, in order to stay ahead.

Current Attack Vectors Show No Signs of Slowing

While novel threats cast a looming shadow, IT leaders must also combat today's most common attack vectors, including

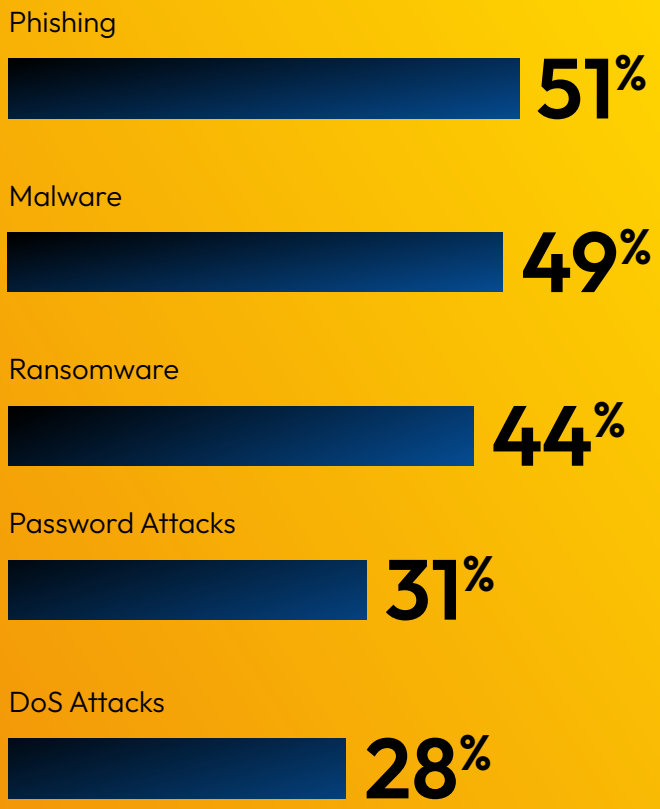
61%	59%	49%	38%	37%
Phishing	Malware	Ransomware	Password Attacks	DoS Attacks

Stolen or weak passwords and credentials remain a leading cause of breaches. Fifty-two percent of survey respondents shared that their company's IT team struggles with frequently stolen passwords, underscoring the importance of creating and safely storing strong, unique passwords for every account.

To stay ahead of breached credentials falling into the hands of bad actors, 72% of companies monitor the dark web for stolen employee credentials. A dark web monitoring service enables organisations to stay abreast of account information and take action immediately if credentials are found to be compromised. Adopting a dedicated password manager can help address both issues head-on, offering the highest level of encryption and features like dark web scans and alerting.

KEEPER

Cyber attacks that are increasing, according to IT leaders



Today, an overwhelming 67% of companies struggle to combat phishing attacks. The explosion in AI tools has intensified this problem by increasing the believability of phishing scams and enabling cybercriminals to deploy them at scale. Eighty-four percent of respondents said that phishing and smishing have become more difficult to detect with the rise in popularity of AI-powered tools and revealed that AI-powered phishing is their top concern (42%) when it comes to AI security.

Who is behind the attacks - and who is at the greatest risk?

Today, the top three most common sources of cyber attacks include:

Independent Hackers

Hacktivist Groups

Corporate Espionage Agents

While many attacks stem from independent hackers or hacktivist groups thousands of miles away, they can also happen in an organisation's own backyard: **40% of survey respondents shared that they have experienced a cyber attack that originated from an employee.** This underscores the importance of deploying technology that prevents both intentional and unintentional insider threats.

A Privileged Access Management (PAM) solution helps IT administrators and security personnel manage and secure privileged credentials and enforce the principle of least privilege. If a cybercriminal does gain access to an organisation's networks, PAM platforms minimise the blast radius by preventing lateral movement.

Who faces the greatest risk from external threats? Cybercriminals are enticed by monetary transactions and sensitive personal information that can be exploited from certain industries.

The barrage of attacks today's IT leaders must combat highlight the need for proactive cybersecurity strategies that can adeptly counter both existing and burgeoning threat vectors.

The top three most frequently hacked industries include:

Hospitality/Travel

Attacks happen weekly, with ransomware and malware being the most common types of cyber attack

Manufacturing

Attacks happen weekly, with phishing and malware being the most common types of cyber attack

Financial Services

Attacks happen monthly, with phishing and malware being the most common types of cyber attack

Conclusion

Attacks are changing but fundamental cybersecurity best practices are not

Keeper's research illuminates the new and novel ways attackers are wreaking havoc on today's enterprises, mid market organisations and small businesses. With AI-powered attacks at the helm, the tools in cybercriminals' arsenals are growing more sophisticated. As technology continues to advance, fighting evolving threats requires constant adaptation.

Despite this ever-evolving threat landscape, the fundamental rules of protecting an organisation in the digital landscape remain relevant. Organisations should prioritise adoption of solutions that prevent the most prevalent cyber attacks, including password and PAM solutions. A password manager can mitigate risks by enforcing strong password practices, while PAM safeguards an organisation's vital assets by controlling and monitoring high-level access, collectively fortifying defences and minimising potential damage in the event that a successful cyber attack does occur. Integrating these solutions creates a layered security approach that stands the test of time – restricting unauthorised access and enhancing overall cybersecurity resilience – **now and in the future.**