Cyber Security Trends - 2024

Summary

The state of cybersecurity in 2024 reflects a dynamic and complex landscape shaped by technological advancements, evolving threats, and increased awareness of cyber risks. Overall, cybersecurity in 2024 is expected to be marked by an arms race between sophisticated attackers and defenders, with technology like Generative AI playing a central role on both sides. Organizations must adapt to these challenges through technological innovation, regulatory compliance, workforce development, and an overarching focus on resilience and risk management.

Threat Trends in 2024

- Advanced Threats & Attack Techniques
- Cyber Threats Targeting U.S. Elections
- Cloud Security Becomes More Essential
- Email Attacks Expected to Increase
- Account Compromise in Focus

Cybersecurity Trends

- Regulatory & Compliance Challenges
- Cybersecurity Skills Gap
- Enhanced Cybersecurity Technologies

Threat Trends in 2024

Advanced Threats & Attack Techniques

Cyber threats have continued to advance, becoming more sophisticated and leveraging advanced techniques like artificial intelligence (AI), large language models (LLM), and machine learning for targeted attacks. AI and LLMs power tools like ChatGPT, but can also be utilized in phishing, smishing, and other social engineering operations to make the content and material appear more legitimate. Misspellings, grammar errors, and lack of cultural context will be harder to spot in phishing emails and messages. LLMs will allow an attacker to create legitimate content, and generate a modified version that looks, flows, and reads like the original, but suits the attacker's goals.

Protection Steps

- Implement AI-powered threat detection systems to analyze patterns and predict potential threats.
- Keep all software and systems updated with the latest patches. Attackers using AI can quickly find and exploit vulnerabilities, so closing these security gaps promptly is crucial.
- Educate employees about the latest cybersecurity threats, including AI-driven attacks.
- Implement strong authentication measures, such as multi-factor authentication. AI attacks often try to exploit weak authentication systems.

AI-targeted attacks are sophisticated and constantly evolving. Therefore, adopting a dynamic and proactive approach to cybersecurity is crucial, as well as continually adapting and updating your strategies to counter these advanced threats.

Cyber Threats Targeting U.S. Elections

As the United States gears up for a presidential election, it is anticipated that various national entities and malicious cyber actors will engage in diverse cyber activities. These activities could range from espionage to influence campaigns aimed at the election infrastructure. They might also involve fake social media representations of political candidates and strategic information campaigns to influence voters. Post-election, a decline in these operations is not expected. In fact, there might be a rise in targeted attacks such as spear phishing, particularly against the U.S. government. Countries like China, Russia, and Iran might intensify their efforts to secure a strategic advantage, possibly during a transition of administrations. Throughout 2024, these campaigns are expected to become more widespread and efficient, partly due to the enhanced capabilities provided by generative AI technologies, which can amplify the scale and pace of such operations.

The impact from these attacks could range from social disruptions and election related disruptions to infrastructure disruptions and broader outages.

Cloud Security Becomes More Essential

With the widespread adoption of cloud computing, there's a heightened focus on cloud security. Organizations are shifting to hybrid and multi-cloud environments, increasing the complexity of security management. While cloud computing has made business systems much more accessible to users, it also makes it much easier for bad actors to attack these systems. This makes proper cloud security essential for every business.

The continuation and expansion of remote work models post-pandemic have made cloud services essential for day-to-day operations. This distributed access to business resources increases the potential for security vulnerabilities, making cloud security crucial for protecting remote work environments. As more businesses undergo digital transformation, the adoption of cloud services has surged. With critical business operations and sensitive data increasingly hosted in the cloud, ensuring robust security is paramount to protect against data breaches and cyber threats.

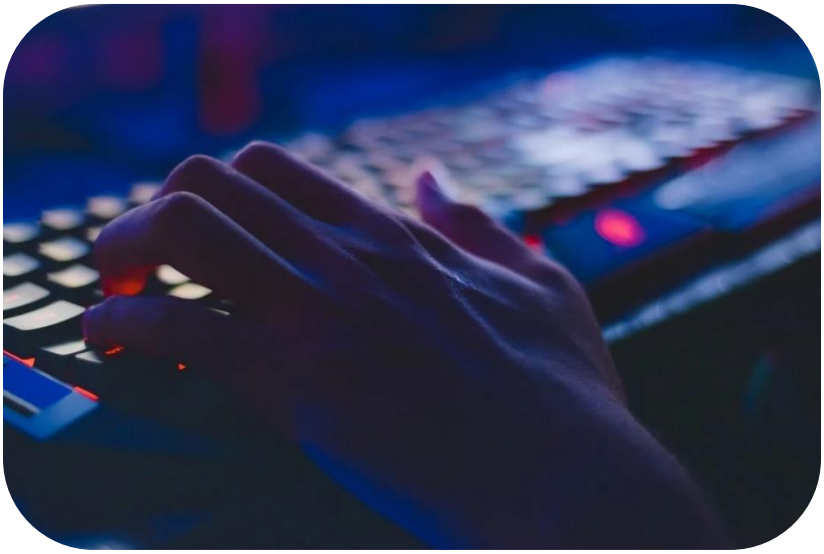
Protection Steps

- Implement Strong Access Controls using MFA and Role-Based Access Controls
- Ensure sensitive data is encrypted in transit and at rest.
- Educate your employees about cloud security best practices and the importance of following security protocols.
- Perform Regular Security and Compliance Checks for security vulnerabilities.

In essence, the significance of cloud security in 2024 is driven by the increasing reliance on cloud services, evolving cyber threats, regulatory pressures, and the need to protect a growing, interconnected digital ecosystem. Businesses must continuously adapt and enhance their cloud security strategies to navigate these challenges effectively.

Account Compromise in Focus

The widespread reliance on usernames and passwords for authentication and access control has repeatedly led to vulnerabilities due to compromised credentials. Data breach analyses frequently pinpoint these compromised credentials as the primary attack vectors. According to a study by the Identity Defined Security Alliance (IDSA), breaches stemming from credential issues are both widespread (with 94% of respondents having faced an identity-related attack) and largely preventable (99%).



However, many organizations still lack crucial security measures related to identity management. Those who have established proper access controls often overlook the growing number of non-human identities that emerge from digital initiatives like DevOps, cloud transformations, and the Internet of Things. Consequently, both human and non-human identity compromises are anticipated to be a key driver of cyberattacks in 2024.

Protection Steps

- MFA adds an extra layer of security by requiring additional verification beyond just a password. Focus on strong MFA such as phishing-resistant MFA or Fast Identity Online 2 (FIDO2) security keys. FIDO2 is a set of technology standards aimed at enhancing the security of online credentials and reducing the reliance on passwords.
- Set up security systems to monitor unusual account activity, such as logins from unfamiliar locations or devices, which could indicate a compromise.
- Use email security tools that can detect and filter phishing attempts, malicious attachments, and suspicious links. Encourage users to verify unexpected requests for sensitive information, even if they appear to come from a legitimate source.
- Advise against using unsecured public Wi-Fi networks to access sensitive accounts or conduct transactions.

By taking appropriate precautions, organizations can significantly reduce the risk of account compromises and enhance their overall security posture.

Cybersecurity Trends

Regulatory & Compliance Challenges

The growing awareness among governments and organizations about the threats to national security and economic stability from cyber-attacks is becoming more pronounced. The societal and political repercussions of widespread data breaches also drive the introduction of new cyber security regulations.

Businesses in the UK are required to comply with the Product Security and Telecommunications Act by April 2024. This legislation mandates minimum security standards for networked products, such as prohibiting the use of default passwords. While implementing the EU's analogous Radio Equipment Directive has been postponed to 2025, this topic will remain a key focus for lawmakers throughout 2024.

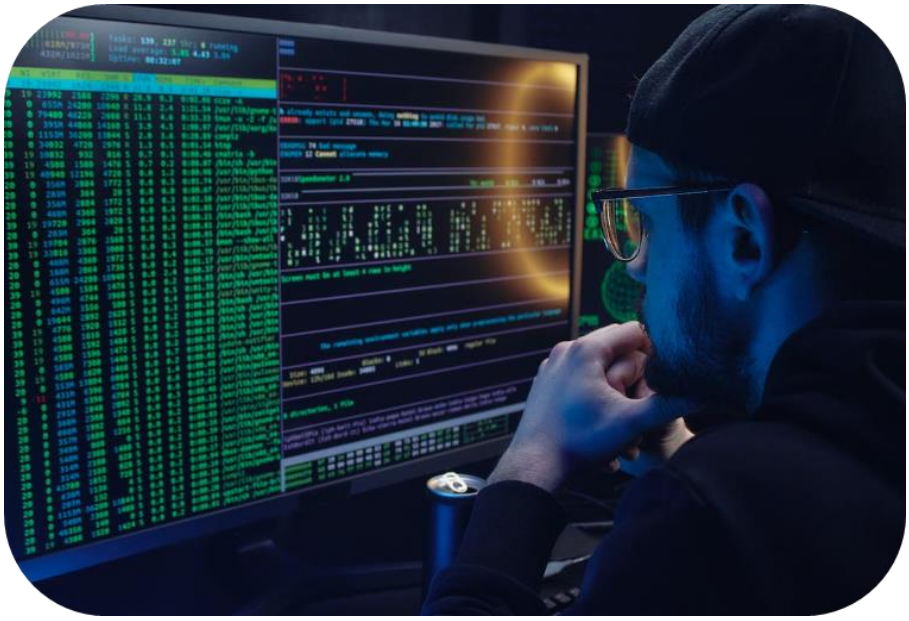
In 2024, the SEC is expected to establish a legal benchmark for inadequate cybersecurity management and delayed reporting of significant incidents. This new legal standard will specifically assign accountability and corresponding penalties to Chief Information Security Officers (CISOs) and Chief Executive Officers (CEOs) for non-compliance. The SEC will pursue litigation and aim to impose substantial penalties. Once established, this legal precedent will likely influence future regulatory enforcement and shape how organizations approach compliance, fully aware of the repercussions of rule violations.

Publicly traded companies must invest more in compliance and cyber security hygiene to avoid hefty fines and reputational damage. But even non-publicly traded companies will likely see increased contractual requirements from customers. Cyber insurance premiums will most likely rise due to these new requirements.

Cybersecurity Skills Gap

The ongoing scarcity of skilled cybersecurity professionals remains a critical issue in 2024. The demand for skilled cybersecurity professionals outpaces supply, leading to a significant skills gap. Many experts in the field believe that the skills gap has further widened throughout 2023, with no sign of changing in 2024.

According to a CompTIA Survey in 2023, there were more than 660,000 cybersecurity job postings in the United States between May 2022 and April 2023. That marks a 28% increase from the same time period in 2020 during the pandemic.



Strategies such as raising salaries and investing in training, development, and upskilling programs are being implemented to address this challenge. However, organizations should persistently seek fresh cybersecurity talent. Another effective strategy is seeking out trusted IT partners to assist with cybersecurity efforts.

Enhanced Cybersecurity Technologies

While Artificial Intelligence (AI) is expected to be used by attackers, it will also assist cyber security teams in identifying, avoiding, or mitigating threats through the use of real-time anomaly detection, intelligent authentication, and automated incident response systems. These newer AI technologies are being integrated into security systems for predictive analytics and automated threat detection and response.

Vendors like Microsoft and CrowdStrike are rapidly building new security solutions that use AI to accurately detect threats from phishing emails, ransomware, and hackers and block them in real time.

It will be critical for businesses to leverage these newer advanced technologies to defend against newer technologies used by attackers.