Cybersecurity Trends 2024

M. R. Pamidi, Ph. D. Editor-in-Chief
Matt Pamidi Creative Director
IT Newswire

December 20, 2023

Cybersecurity is a constantly evolving field that faces new challenges and opportunities every year and 2024 will be no different: Hacksters (**hack**ers + fraud**sters**) will, as usual, a few steps ahead of cybersecurity personeel and the catch-up will continue.

Some of the cybersecurity trends for 2024 are:

- **Cyberattacks on cannabis retailers***:* The legalization of cannabis in some states will create a new market for cybercriminals, as cannabis retailers store large amounts of cash and customer data, and may have weak security systems and compliance standards.

- **Election year disinformation**: Cybercriminals will exploit political tensions and social divisions to spread misinformation and influence public opinion, using advanced social engineering and AI-based techniques.

- **Escalation of ransomware attacks**: Ransomware, a type of malware that encrypts the victim's data and demands a ransom for its release, will continue to be a major threat to businesses and organizations, as attackers target more critical and sensitive sectors, such as healthcare, education, and government.*Rise of AI in cybersecurity:* AI will play a bigger role in both defending and attacking digital systems, as it can automate tasks, analyze data, and predict threats.

- **FEMACyber Insurance:** The Federal Emergency Management Agency (FEMA) may launch a cyber insurance program that will provide financial assistance and recovery services for victims of cyberattacks, similar to its existing programs for natural disasters.

- **National U.S. Data Privacy Act**: The U.S. may enact a federal data privacy law that will harmonize the existing state-level regulations and provide more protection and control for consumers over their personal data.

- **Persistent risk of the remote workforce**: The shift to remote work due to the COVID-19 pandemic has increased the exposure of enterprise data and networks to cyberattacks, as employees use personal devices and home networks that may lack adequate security measures.

- **Zero Trust elevates to boardroom status**: Zero trust, a security model that assumes no trust for any entity inside or outside the network, will become a strategic priority for enterprises, as they seek to reduce the attack surface and mitigate the risks of data breaches.