ORION FORUM

2024 Cybersecurity Year in Review: Notable Facts and Policies

JANUARY 7, 2025

The past year stands out as one in which cyber adversaries have notably increased their operational capabilities. Cybersecurity in 2024 has been marked by the impact of AI, political and military conflicts in cyberspace, and compromised supply chains. Furthermore, nation-state actors have become more aggressive in cyberespionage campaigns, and Advanced Persistent Threat (APT) groups have exploited zero-day vulnerabilities in high-profile cyberattacks. This article reviews the major cyber incidents, the threat landscape, and cybersecurity policies and strategies in 2024.

It is not surprising that cyberattacks are becoming more sophisticated and frequent every year, for cybercrime is profitable for criminal enterprises, who invest in expanding their cybercrime capacity. As *Police Chief Magazine* observes, "Organized crime has gone high tech." Via ransomware attacks or other ways of disrupting business activities, criminals demand large amounts of payment from their victims in exchange for stopping their attacks. For instance, Changed Healthcare, targeted by the Blackcat/ALPHV ransomware group earlier this year, paid $22 million in ransom, while an unnamed Fortune 50 company reportedly paid a shocking $75 million to the Dark Angels ransomware group. Despite the FBI's advice against paying a ransom to threat actors, many companies keep doing so on the premise that the potential damage to their businesses would outweigh the costs of the ransom. This encourages cybercriminals to increase their ransomware attacks.

According to an online zero-day vulnerabilities database, 92 zero-days were identified in 2024 alone, a slight decrease from 2023, in which 98 were discovered. Although a patch has been released for most of the detected vulnerabilities, not all clients patch their systems on day one, remaining vulnerable and prone to opportunistic attacks from threat actors.

On an international scale, Chinese and Russian threat actors reportedly engaged in several cases of cyberespionage and malign influence during 2024. As listed in the database of significant cybersecurity incidents maintained by the Center for Strategic & International Studies (CSIS), Chinese hackers have breached Canadian government networks as well as devices belonging to members of Parliament, hacked cell phones of Trump-Vance and Harris-Walz campaign members, exfiltrated data from Thai government agencies, carried out cyberespionage activities against several Middle Eastern government entities, and attacked and exposed military information from Britain's Ministry of Defense. The list does not end here. In addition, Australia, the United States, Canada, the United Kingdom, Germany, Japan, South Korea, New Zealand, and the Netherlands have accused Chinese hackers of cyberespionage, showing how widespread and alarming such activities were in 2024.

Militarily, the ongoing conflict between Russia and Ukraine has involved cyber-operations on both sides. Since the beginning of the conflict, Russia has launched cyberattacks against several Ukrainian critical infrastructures, government agencies, and businesses to diminish Ukrainian defense and morale, attacks that continued in 2024. Moreover, Russia has extended its cyber-operations to other European countries within the last year, leading Poland, the Czech Republic, and Germany to accuse Russia of targeting government agencies, infrastructure networks, or political entities.

As the 2024 report on the cybersecurity posture of the United States confirms, the activities of Chinese and Russian cyber-threat actors pose a major menace. On the one hand, the Russian Foreign Intelligence Service (SVR) is accused of supply chain exploitation; on the other, China is charged with targeting US critical infrastructure to augment its geopolitical objectives. The 2024 report further alleges that "the PRC, in particular, remains the most active and persistent cyber threat to U.S. Government, private sector, and critical infrastructure networks." The report also highlights current efforts in implementing the national cybersecurity strategy released in March 2023, reasserting the importance of public-private collaboration, particularly in protecting critical infrastructure, modernizing legacy systems across the Federal enterprise, and strengthening the cybersecurity workforce.

Apart from the growing threats and threat actors, several positive developments have nevertheless occurred in cybersecurity. In August, the National Institute of Standards and Technology (NIST) approved three post-quantum cryptography algorithms that can resist cryptographic attacks from quantum computers. In another development, the security of Internet of Things (IoT) devices came to the forefront in 2024, with the EU Cyber Resilience Act set to enter into force in December this year. Furthermore, the US Federal Communications Commission (FCC) adopted rules for the IoT Cybersecurity Labeling program earlier this year. These two initiatives will foster the security of smart devices and encourage the adoption of high-security standards.

Recent trends, however, indicate that ransomware and supply-chain attacks will remain top threats in 2025. As Trend Micro's security predictions report for 2025 anticipates, "ransomware groups will double down on exploiting widely used legitimate tools and applications" to evade detection, thus suggesting a shift from earlier techniques that primarily relied on phishing campaigns. Moreover, Kaspersky's predictions for 2025 include supply chain attacks that target open-source ecosystems. In addition, a growing concern in the cybersecurity community is the use of AI by malicious actors. As Google's cybersecurity report forecasts, attackers will use AI tools and deepfakes to improve their social engineering attacks, identity theft, and fraud.

On an optimistic note, however, Zero-Trust is expected to gain widespread adoption. AI and ML technologies will continue to enhance cybersecurity systems, particularly in threat detection. Additionally, we are likely to see greater collaboration between the government and the private sector. The importance of cybersecurity has reached a level that cannot be overlooked. Cybersecurity matters for individuals, organizations, businesses, and nations, and it will only grow more vital in the coming years.

Orion Policy Institute (OPI) is an independent, non-profit, tax-exempt think tank focusing on a broad range of issues at the local, national, and global levels. OPI does not take institutional policy positions. Accordingly, all views, positions, and conclusions represented herein should

be understood to be solely those of the author(s) and do not necessarily reflect the views of OPI.