Five big cybersecurity trends for 2024

Gain key insights to help protect your organization in the coming year.

Google Cloud

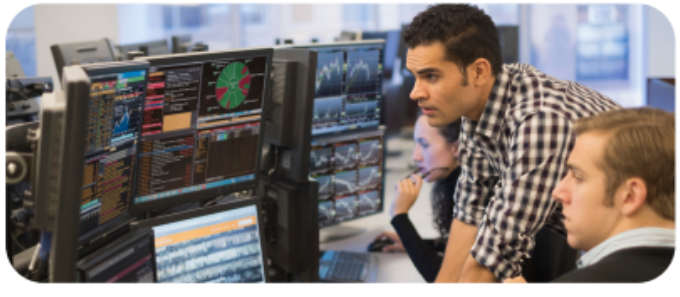
Trend 1

AI will have a major impact on cyber operations and security.

More convincing and scalable phishing campaigns

Phishing and SMS threats could be harder to spot with fewer misspellings and grammar errors.

With access to info like names, companies, and job titles, attackers could use AI to more easily target more people with personal emails tailored to them.



More skepticism in media

A clever AI prompt will be all attackers need to create fake news, deepfake photos and videos, fake phone calls, and more. As this content enters the news cycle, people may become less trustful of news and info they see online.

AI-powered attacks will be met with AI-powered defenses

With AI, organizations will be able to strengthen and expedite their detection and response. Defenders will also be able to analyze large data sets faster to gain the insights they need to take immediate action.

Trend 2

Nation states will conduct cyber operations for geopolitical gains.

China

Cyber activity from China is expected to continue to be driven by long-term territorial goals, regional issues, and economic influence over key markets.

North Korea

North Korea is expected to continue to place heavy emphasis on conducting cyber crime, notably targeting cryptocurrency, to fund espionage operations as well as their weapons and nuclear program.

Iran

Priorities including geopolitical ambitions, economic development needs, and competition with regional rivals will be key drivers of Iran's state-sponsored cyber activity in 2024.

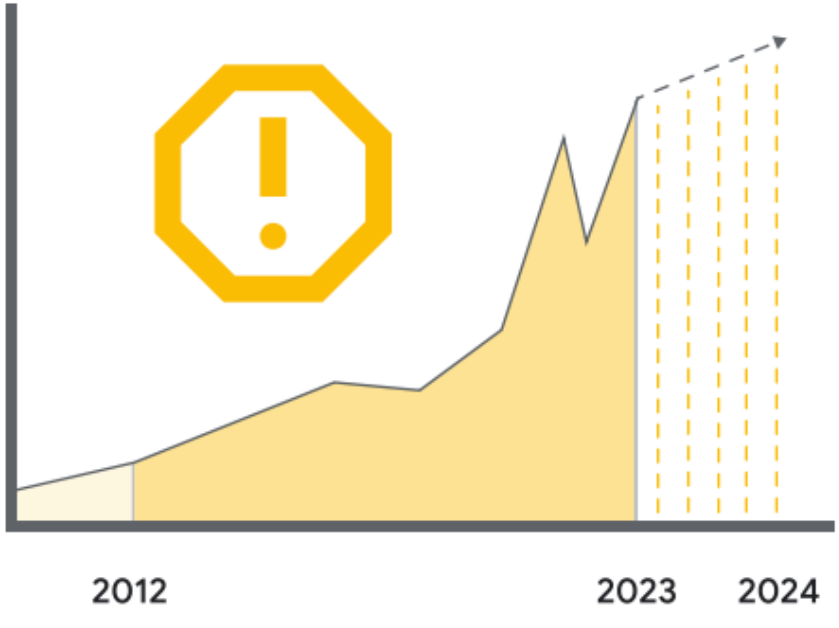
Russia

Along with intelligence gathering and disruptive attacks focusing on Ukraine, there could be more cyber espionage consistent with Russia's long-term geopolitical goals, as well as IP theft.

Trend 3

There will be more zero-day attacks and use of other techniques to evade detection.

Zero-day attacks are rising.



There's been a steady increase in zero-day attacks since 2012, with 2023 on track to beat the previous record set in 2021. In 2024, we expect more zero-day attacks by both nation-state attackers and cyber criminal groups.

Why?

Attackers want access to an environment for as long as possible. By exploiting zero-day vulnerabilities, they can maintain access for much longer than if they were to deploy malware.

We also anticipate:

- More targeting of hard-to-monitor edge devices and virtualization software
- A revival of older attack techniques that modern detection systems may not account for
- Espionage groups to create "sleeper botnets" out of vulnerable Internet of Things, end-of-life devices, and routers

Trend 4

There will be a rise in cyber activity around major global events.

In addition to rising hacktivism related to ongoing conflicts, it's likely that attackers will use a range of techniques to target elections around the world and the Summer Olympics in Paris.

For the upcoming U.S. presidential election, we expect cyber activity such as espionage and influence operations targeting electoral systems.

We also anticipate seeing similar cyber activity around European Parliament elections, as well as elections taking place in Taiwan, South Korea, India, and Indonesia.

Trend 5

The way malware is developed will change.

Malware authors are expected to continue developing malware in modern programming languages such as Go, Rust, and Swift. These languages and ecosystems enable fast development of complex malware that's cheaper to write and harder to detect.