4 Key Cybersecurity Trends to Watch in 2024

SANS | GIAC CERTIFICATIONS

Organizations are set to face both new and familiar cybersecurity challenges in 2024. While CISOs will continue to deal with the volatility that comes with more attacks and vulnerabilities, they will also face new challenges that require them to operate in a more proactive and calculated manner. Four major trends will bubble to the surface this year, presenting CISOs not just with challenges but with opportunities to empower their organizations and security teams. Each of the trends outlined in this infographic are covered in greater detail and paired with actionable guidance in the 2024 SANS white paper, SANS CISO Primer: 4 Cyber Trends That Will Move the Needle in 2024.

The State of Cyber in 2024

$4.45 MILLION

The global average cost of a data breach

277 DAYS

Average data breach lifecycle

82%

Share of breaches that involved data stored in cloud environments

1. The Duality of Generative AI: A Source of Risk and Promise

130% PER MONTH

A study from the British non-profit Center for Countering Digital Hate claims that, on average, AI-generated disinformation has risen by an average of **130% per month** on X (formerly Twitter) over the past year.

100,000 MENTIONS

A recent Accenture report revealed over **100,000 mentions** of AI on corporate earnings calls since ChatGPT's release, signaling the start of a massive technology shift across the private sector.

Google's 2024 Cloud Cybersecurity Forecast predicts that GenAI large language models (LLMs) will be utilized to make content appear more legitimate in various cyberattacks such as: phishing, BEC, and other social engineering operations.

Employees who receive **continual training** are 5x more likely to **identify and avoid malicious links**.

**See full whitepaper for CISO best practices for managing GenAI risk

Verizon's DBIR for 2023 found that

74%

of breaches in the past year involved a human element.

Forrester analysts predict GenAI will drive the human error rate to **90%** over the next year.

2. Zero Trust Implementation: The Old but New Security Imperative

Gartner analysts forecast that by 2025,

45%

of organizations worldwide will have experienced attacks on their supply chains, a **three-fold** increase from 2021.

SANS research shows that over

1/3

of organizations have become collateral damage to a third-party cyber incident.

235 DAYS

is the average amount of time that supply chain attacks go unnoticed after the first entry point.

Implementing **continuous zero trust authentication** requires significant security architecture revamps necessitating CISOs to **expand their cybersecurity team capabilities** to avoid compromising security postures.

**See full whitepaper for CISO best practices for implementing zero trust

3. Cloud Security: A Vital Line of Defense

$4.75 MILLION

Nearly **40% of attacks** spanned multiple environments, incurring an above average cost of **$4.75 million** per breach.

MORE THAN 80%

More than **80%** of breaches assessed in IBM's 2023 Cost of a Data Breach Report involved data stored in public or private cloud environments.

24% YoY increase in data privacy and cloud security spending rates. Among all security categories, these two categories are projected to record the highest growth rates in 2024, Gartner predicts.

**See full whitepaper for CISO best practices on cloud security

Maximizing cloud expertise must be a **concrete, planned, and capacity-considered component** of an organization's security team **– not an afterthought**.

4. Cybersecurity Complexity: Maturing Cyber Capability Development

As businesses grow their technology investments, attacker capabilities continue to scale alongside them.

Technological capabilities and rich tooling are available to security teams but are not being leveraged fully.

Increasingly complex environments create more complex capacity and skills needs.

Leaders universally admire a more structured approach to cyber capability development and want to get started in the coming 12-18 months.

It is **crucial** for CISOs to **continually invest in their own teams** – people who know the business, goals, and security environment. Arming them with the **latest knowledge of tools and threats** is a cornerstone to maximizing the return on your security investment.

**See full whitepaper for CISO best practices for reducing complexity

SANS | GIAC CERTIFICATIONS