Build cyber resilience. Reduce your risk.

Understand the top cybersecurity facts, trends, and predictions all executives should know to better secure their organizations against cyber risks.

SOPHOS

Geopolitics

While 2024 marked a historic year of global elections, with nearly half of the world's population going to the polls, broader geopolitical tensions continue to shape the cyber threat landscape into the second half of 2025. The effects of state-aligned cyber activity remain visible, underscoring the importance of vigilance. Organizations should stay informed through timely, contextual threat intelligence to better understand the evolving risk environment and prepare accordingly.

Artificial Intelligence

AI will drive significant enhancements in how organizations secure themselves, but it can also present risk when in the hands of threat actors. Organizations need to educate their teams on the proliferation of deep fakes generated by AI and how cybercriminals are experimenting with large language models (LLMs) to improve their phishing tactics and lures, and share those learnings in forums.

1) Cyber Defense Magazine: The True Cost of Cybercrime: Why Global Damages Could Reach $1.2-$1.5 Trillion by End of Year 2025
2) IBM: Cost of a Data Breach Report 2024
3) Sophos Active Adversary Report 2025
4) FBI Public Service Announcement (September, 2024)

Cost of a data breach

By the end of 2025, cybercrime is predicted to cost the world $1.2 trillion, according to Cybersecurity Ventures.(1) At the organizational level, the global average cost per data breach was $4.8 million USD in 2024 and is only expected to rise, according to an IBM study.(2)

Ransomware

Ransomware remains the primary cyber threat to businesses. In 2024, median dwell time in ransomware attacks studied in Sophos' Active Adversary Report was less than 48 hours, representing a continuous decline year-over-year.(3) Cybercriminals are becoming more smash-and-grab in their approach — stealing what they need and getting out quickly and undetected.

Business email compromise

Business email compromise (BEC) attack totaled losses of more than $55 billion USD between 2013 and 2024.(4) We expect to see ongoing innovation in the methods BEC actors use to evade security defenses and deceive end users, such as QR code phishing attacks and voice phishing (aka "vishing").

Cybersecurity Disclosure Regulations

In December 2023, the U.S. Securities and Exchange Commission (SEC) implemented a new Cybersecurity Disclosure Rule requiring public companies to disclose any cyber incident with a "material" impact within four business days. While this rule specifically applies to U.S.-listed companies, it reflects a broader global trend toward increased regulatory scrutiny and mandatory cyber incident reporting. Organizations worldwide should monitor evolving disclosure requirements in their respective jurisdictions, integrate them into their incident re-

groups, may attempt to exploit such regulations for extortion purposes.

SOPHOS

Cyber Resilience Checklist

- **Get the security basics right**

  Reduce risk by implementing foundational security controls such as multi-factor authentication, vulnerability detection, and patching, along with threat monitoring and detection for all endpoints, network, and cloud resources.

- **Align risk appetite with investments**

  Ensure the proper identification of relevant risks along with the likelihood of business impact. Leverage a control framework that fits your organization's specific needs and threat profile.

- **Avoid a siloed security approach**

  Seek out a solution like extended detection and response (XDR), designed to connect all your best-in-class security solutions through integrations. This will help your organization detect and respond effectively and at scale.

- **Optimize talent and engage partners to close gaps**

  Assess enterprise risk thoroughly by evaluating your depth of talent throughout the entire organization, then consider partnering with a vendor that offers managed detection and response (MDR) services for a hybrid or fully managed SOC that can extend your

- **Create a formal incident response plan and practice**

  Determine how you will respond to a breach, then build out a comprehensive plan. Be sure to validate your approach with tabletop exercises so that you are ready when time is critical.

- **Communicate with your cyber insurer**

  Align with your insurer on your security strategy and add your preferred incident response vendors to your cyber insurance policy. This will help ensure that you are reimbursed in the event of an incident.

To learn how Sophos helps more than 600K organizations secure their operations, visit sophos.com