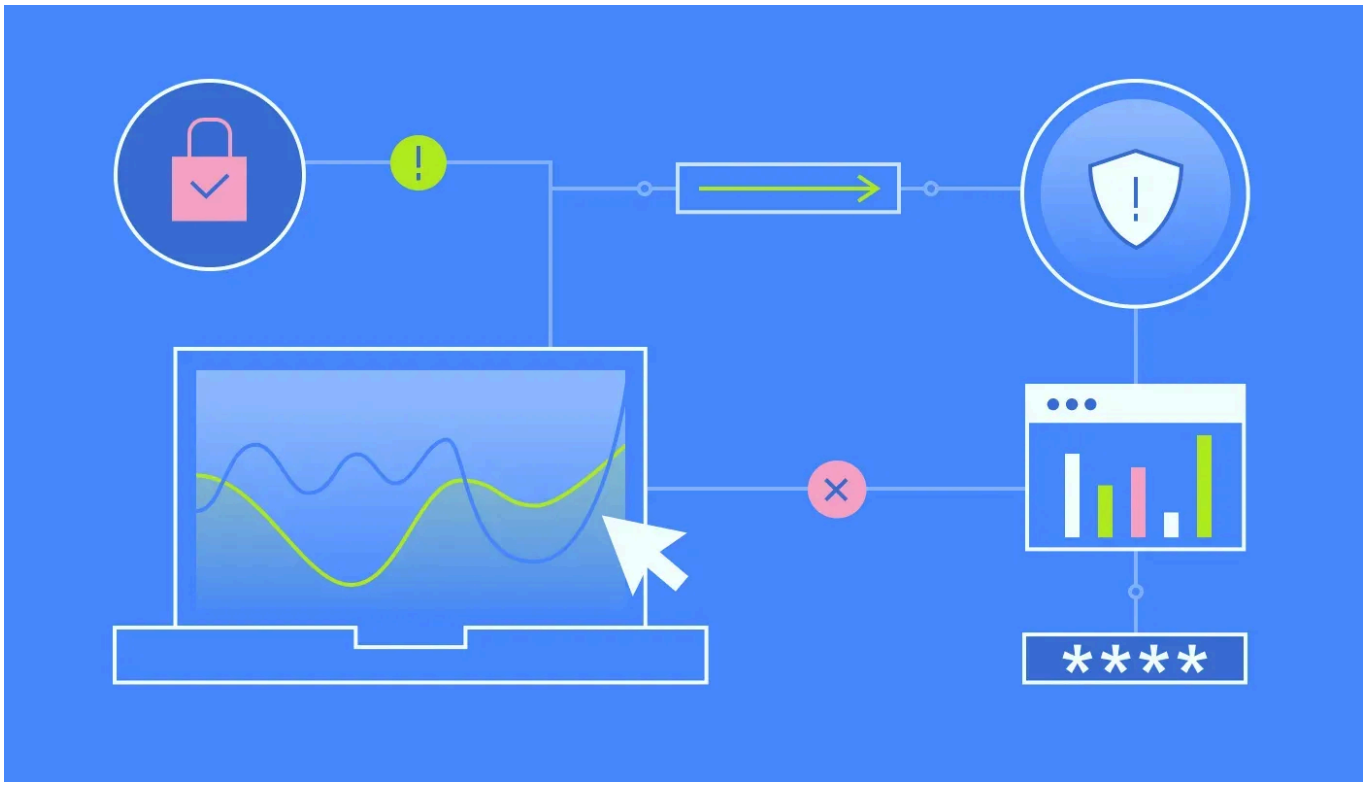
TRENDS & STATISTICS

10 must-know cybersecurity trends for 2025

Joanna Krysińska

Nov 25, 2024 15 min read



> ***Summary:*** *Cybersecurity evolves fast. In 2025, expect quantum threats, AI-driven ransomware, identity breaches, and stronger roles for SOCs and CISOs to combat threats.*

Cybercriminals keep finding new, more sophisticated techniques. The past year has seen even faster changes. Gartner **predicts** that cybersecurity threats, like **quantum computing risks** or **AI-powered ransomware attacks**, will grow in 2025. As companies use more AI to streamline operations, make better decisions, and improve customer experiences, new AI-related risks are also on the rise.

The cost of cybercrime is expected to jump, reaching **$13.82 trillion by 2028**. This adds more pressure on businesses to strengthen defenses against data breaches, fraud, and system disruptions.

In this article, we'll look at key cybersecurity trends for 2025 and discuss ways organizations can tackle these security challenges to protect their sensitive data and systems.

Key takeaways

- Quantum computing could break current encryption methods.

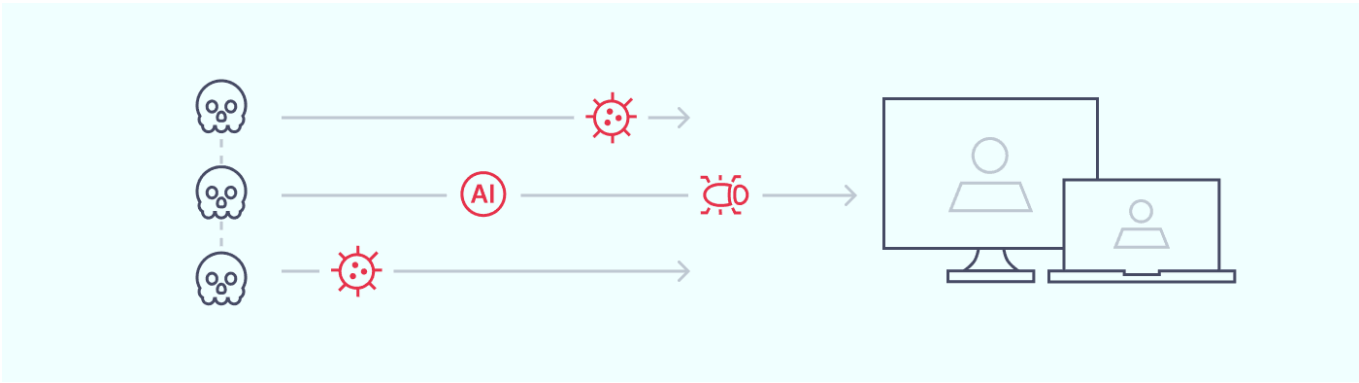
- Cybercriminals will be increasingly using stolen credentials to access systems.
- AI agents will be involved in 25% of data breaches by 2028.
- AI-driven SOC co-pilots will improve threat detection and response.
- CIO and CISO roles will merge to address AI-driven cybersecurity threats.
- Cloud security threats will increase with AI and more complex attacks.
- Securing IoT and multi-cloud environments will be one of the major cybersecurity challenges.

AI-generated ransomware

Ransomware attacks are growing in **frequency and sophistication**. IBM's X-Force Threat Intelligence Index 2024 shows that ransomware groups upgraded their tactics in the past year.

In the Sophos' State of Ransomware 2023 Report, 66% of organizations reported experiencing ransomware attacks. These attacks are getting smarter, with AI helping attackers to quickly scout networks and create more targeted ransom demands.

In 2025, **artificial intelligence (AI) and automation** are expected to make ransomware attacks faster and more accurate. With these advanced techniques, ransomware can spread quickly across networks.



Quantum computing security challenges

Researchers in China have recently announced a breakthrough. They claim to have found a way to break the most common form of online encryption using quantum computers

with just 372 qubits. This is a major milestone in computer security. Experts predict quantum computing could be powerful enough to crack current encryption methods as early as 2025.

While quantum-based attacks are still a few years away, organizations must start preparing *now. They* need to transition to **encryption methods that can resist quantum decryption** and protect their sensitive data from these emerging threats before it's too late.

Cyber threats targeting identities

Attackers always take the easiest route to reach their goals. This year, they have shifted from hacking into systems to ***logging in*** **using valid credentials.** This change is shown in a 71% year-over-year increase in attacks that use legitimate login details.

For the first time in 2024, exploiting valid accounts became the most common system entry point, making up 30% of all incidents. This shows that it's easier for cybercriminals to **steal credentials** than to exploit vulnerabilities or rely on phishing. This **trend is expected to continue** in 2025.

AI agents

By 2028, Gartner predicts that 25% of enterprise breaches will involve AI agents used either by external attackers or malicious insiders. As **AI agents expand the hidden attack**

surface, businesses will need new security measures to protect against both external threats and disgruntled employees who might misuse AI.

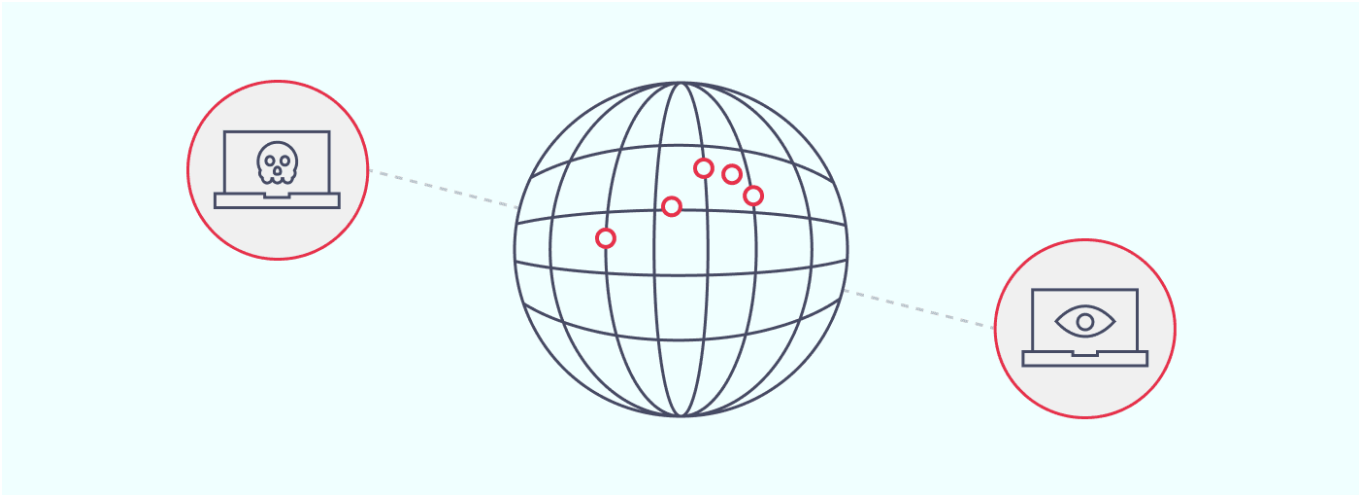
Gartner analyst Daryl Plummer points out that enterprises can't wait to implement controls against AI agent threats. It's far easier to build security into products and software upfront than to add them after a breach. This highlights the need for proactive, AI-focused risk and security solutions in 2025 and beyond.

Political and election-related cyber-attacks

On **Election Day 2024** in the U.S., several DDoS attacks on political and election sites were blocked. Similar attacks were seen in France, the Netherlands, and the U.K. during their elections. The U.S. also experienced a rise in attacks *before* the election.

The Office of the Director of National Intelligence (ODNI), FBI, and the Cybersecurity and Infrastructure Security Agency (CISA) **report** that Russia increased efforts to disrupt the 2024 U.S. elections. Its target was swing states with fake media to create division and doubt. Iran was also involved in cyber-attacks on former President Trump's campaign and attempts to spread misinformation.

Given these cyber threats, upcoming 2025 elections—such as those in Denmark, the U.K., Portugal, and Poland—may face similar risks. This makes **government cybersecurity** a critical focus for protecting democratic processes.



AI-powered SOC co-pilots

By 2025, AI-driven co-pilots will change how Security Operations Centers (SOCs) work. These AI tools will help teams manage large amounts of data from firewalls, system logs, vulnerability reports, and threat intelligence. With AI co-pilots, SOCs can analyze data more efficiently, focus on the most critical threats, and recommend solutions.

AI tools in SOC dashboards will automate key tasks, reduce false alarms, and help security teams respond to incidents faster. The ability to turn large amounts of data into clear, actionable insights will be key for defending against advanced cyber-attacks.

AI-driven SOC co-pilots will impact the industry in 2025, helping security teams prioritize threats and transform overwhelming data into valuable intelligence, **improving SOC efficiency.**

CIO and CISO roles merge as AI adoption increases

As companies use more AI and hybrid cloud systems, **the roles of CIO and CISO will merge**. This will lead to a more integrated approach to risk management. In 2025, CIOs will take on a bigger role in managing cybersecurity, creating stronger alignment between IT and security teams.

By working together, IT and security teams can develop a shared strategy that balances new technology with solid security measures. This trend is key for keeping business operations secure in an AI-driven environment.

New security regulations

In 2024, regulators introduced new cybersecurity and privacy policies to address risks tied to technologies like generative AI (genAI) and third-party relationships. Security and risk leaders worked quickly to secure genAI despite its evolving use cases. Many industries faced IT disruptions due to poor resilience planning, and software supply chain breaches increased as third-party risks were underestimated.

As we mentioned, cybercrime costs are expected to surge dramatically in 2025. **Regulators will take a stronger stance on protecting consumer data**. Organizations will shift toward more proactive security measures to reduce the impact of cyber threats. Forrester's 2025 predictions stress the need for organizations to adapt to these new risk challenges.

Cloud security

As more businesses move to the cloud, securing these environments is more critical than ever. In 2025, cloud security will face new threats, such as data breaches, misconfigured settings, insider threats, insecure APIs, DDoS attacks, inadequate data backups, and compliance violations.

Cybercriminals will also **use AI to automate attacks on cloud systems**. This means businesses must shift from fixing issues after they happen to preventing them upfront. The speed and complexity of attacks will require companies to build security systems that can detect and stop these threats early.

Businesses must implement encryption, monitor cloud configurations, train staff, secure APIs, deploy DDoS protection, maintain robust backup systems, and ensure compliance with regulations like GDPR and HIPAA.

Internet of things (IoT) and cloud security challenges

The rise of IoT devices and the shift to cloud platforms are increasing cyber risks. By 2025, over 90% of companies will use multiple cloud platforms, and the number of IoT devices will exceed 32 billion.

While cloud providers offer strong security, managing multiple platforms creates vulnerabilities, especially with misconfigurations or poor monitoring. Many IoT devices, like smart home tech and sensors, lack proper security, making them easy targets for bad actors.

The growth of IoT will increase the need for secure cloud storage, real-time processing, and cost-effective scalability. **Misconfigurations and insecure APIs** will remain top targets, making system security a major challenge in 2025.

Strategies for business safety in 2025

Keeping your business safe in 2025 means using a layered defense. Focus not only on innovative technology but also on planning and regular training. As cyber threats get smarter, here are practical steps to protect your systems, data, and networks.

1. Use multi-factor authentication (MFA) to regulate network access.
2. To prevent ransomware from penetrating your systems, use a mix of firewalls and threat protection.
3. Assign minimal user privileges in line with Zero Trust principles.
4. Secure remote devices with VPNs.
5. Use a password manager for strong passwords.
6. Encrypt your sensitive data.
7. Use data loss prevention (DLP) tools to track valuable data.
8. Use intrusion detection systems/intrusion prevention systems (IDS/IPS) to track threats in depth.
9. Back up data regularly.
10. Audit backups and threat responses to ensure quick disaster recovery.
11. Regularly test your security systems.
12. Risk assess core threats and create response plans.
13. Train all staff to detect phishing attacks.

To sum up, 2025 will bring new and complex cybersecurity challenges. Quantum computing, AI-driven attacks, and identity breaches will demand new defenses. Businesses need a clear strategy, using tools like multi-factor authentication, encryption, and threat detection.

Merging the CIO and CISO roles will also help companies with stronger security. Regular testing, training, and a well-planned response strategy will be essential to manage these evolving risks and protect data, systems, and operations. These steps will help protect data, systems, and business operations from new risks.

Joanna Krysińska

Senior Copywriter

A writer, tech enthusiast, dog walker, and amateur pastry chef, Joanna grew up in a family of engineers and mathematicians, so a techy mind is in her genes. She loves making complex tech topics less complex and digestible. She also has a keen interest in the mechanics of cybercrime.

Share this post

Related Articles

NordLayer®