



Cyber risks, current trends and predictions for 2025 and beyond

19th September 2025

Ankur Gupta

Sudeep Pandey

Agenda

Major cyber risks and challenges in a nutshell

01

AI perspectives between hype, risks and advancements

03

02

Geopolitics

Business email compromise (BEC) and Business Communication Compromise (BCC)

05

04

Ransomware trends

Data, privacy & cybersecurity regulation

07

06

Supply Chains remain weak spot

Cyber Risk Management predictions

09

08

Personal Lines – trends and developments

10

Trends and outlook on Cyber Insurance

Major cyber risks and challenges in a nutshell

Top challenges of today and tomorrow



Major cyber risks and challenges in a nutshell

Top challenges of today and tomorrow and the effects



Effects

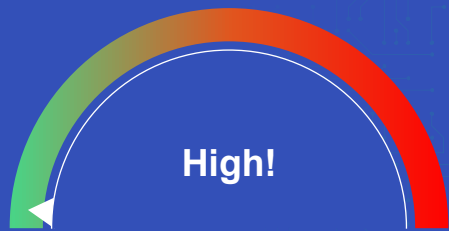
- Higher cyber exposures for organizations
- Expected increase in frequency and severity of losses
- More demand for cyber insurance

Geopolitical tensions have affected the cybersecurity strategy for nearly 60% of organizations. While some have modified their insurance policies, a significant portion have changed vendors, trading policies, or ceased business altogether in certain countries.

— WEF
“The Global Cybersecurity Outlook 2025”

- Tense geopolitical situation will further impact tech investments, innovation and also tech related nationalism
- Bans of certain vendors and third party's software will be more common
- AI- and privacy related regulation will be balanced to not disable innovation but also to protect societies and focus on national security interests
- Disinformation and unverified AI-generated content will remain an important part of hybrid warfare bringing political systems and societies
- Reported cyber attacks between 01/2023 and 01/2024 highlighted that global critical infrastructure faced over 420 million cyberattacks. U.S. was the primary target, but 163 other countries experienced attacks as well (KnowBe4, “Cyber Attacks on Infrastructure - The New Geopolitical Weapon”)

Impact on cyber insurance



- High impact due to sophistication of actors
- AI will add a new layer of geopolitical powerplay
- Cyber arms race heavily influences supply chain and other cyber risks

China

Focus on Taiwan.
The strategic hegemonial race with the U.S. will expand aggressive cyber programs with highest degree of sophistication.

Russia

Cyber espionage and hybrid warfare with strong disinformation campaigns against Ukraine, NATO countries and Europe.

Iran

Usage of cyber program to repress opponents.
Israel-Hamas conflict will continue to dominate Iran's cyber threat activity.

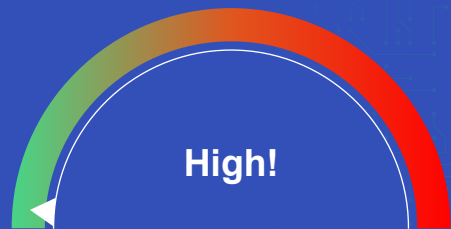
North Korea

Revenue generation through cybercrime and espionage operations.
Strategy with more focus on supply chain compromises.

Others

Geopolitical ambitions and new eras of digital competition brought significant investments into offensive/defensive cyber capabilities for countries like Saudi-Arabia, UAE or Indonesia/ Southeast Asia.

Impact on cyber insurance



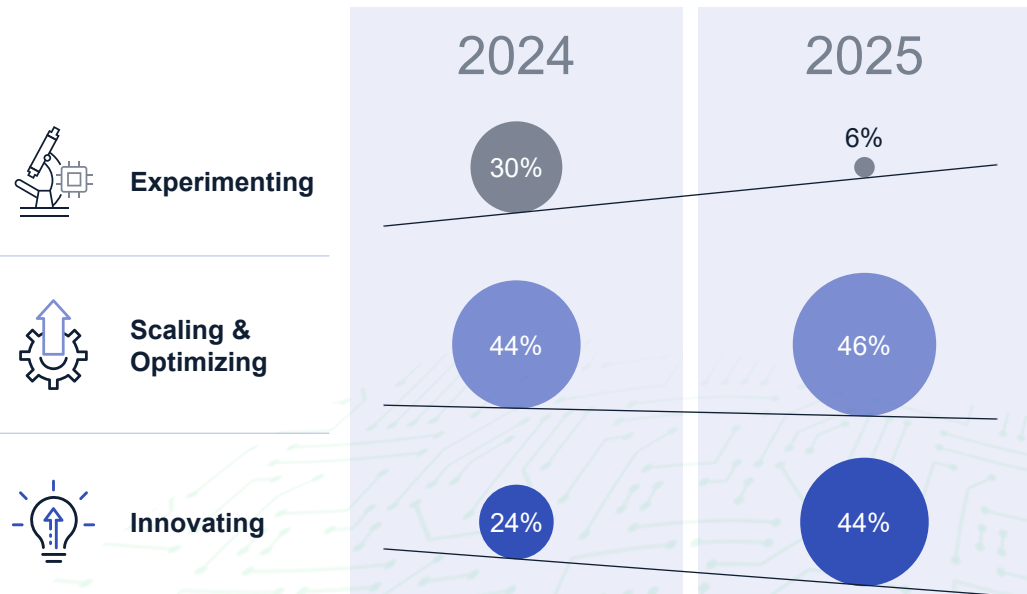
- Race for zero-day vulnerabilities
- Strong research activities
- Collaboration of nation states and APT Groups that dually engage in cybercrime and cyber espionage will further mirror regional and global conflicts

AI perspectives between hype, risks and advancements

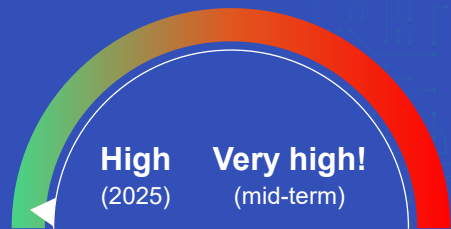
AI will generate a cumulative global impact of \$19.9 trillion by 2030; the potential is great, but the risks are significant.

IDC

“The Global Impact of Artificial Intelligence on the Economy and Jobs”



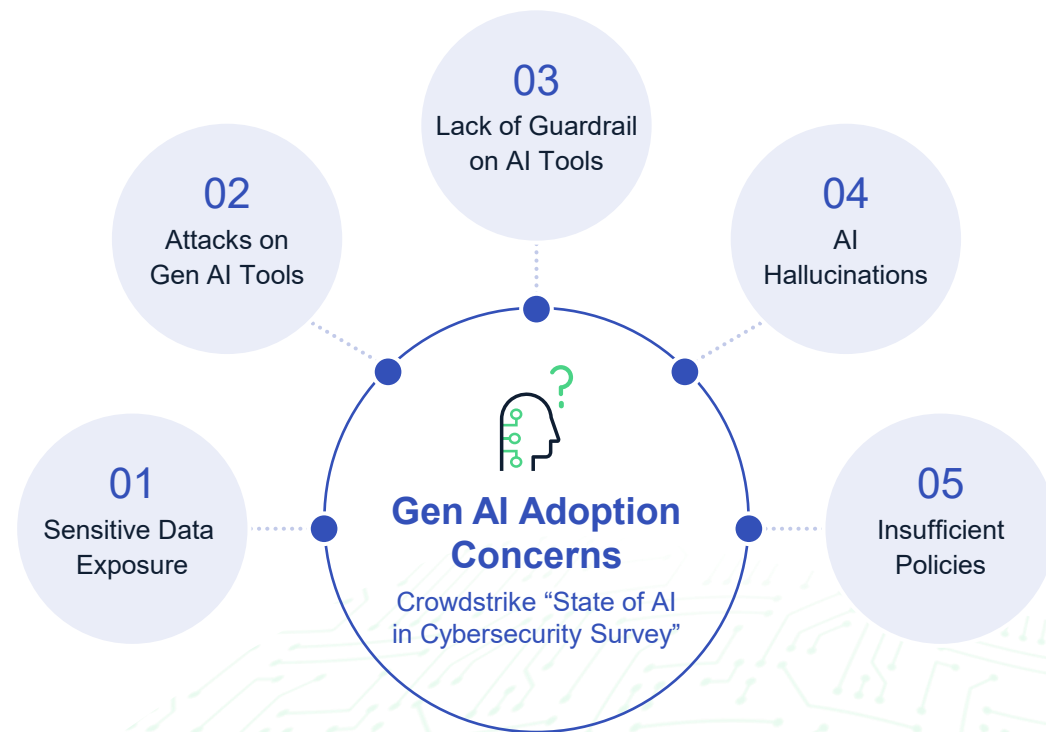
Impact on cyber insurance



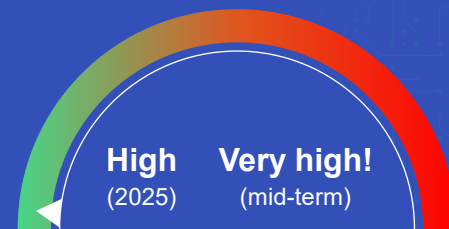
- Increasing usage of AI within the insurance industry
- AI divide in access to AI technologies between individuals, organizations and nation states to expect

AI perspectives between hype, risks and advancements

The applicant's side!



Impact on cyber insurance



- All risk owner & threat actors will be increasingly augmented with AI capabilities
- Democratization of TTP's will lower barriers for access to cybercrime scene
- Frequency of claims expected to rise
- Discussion about "Silent AI" will gather momentum

AI perspectives between hype, risks and advancement

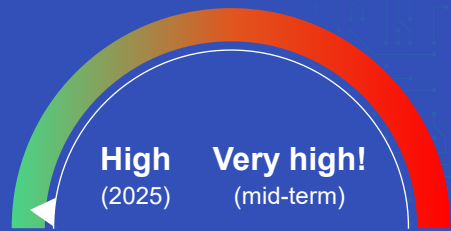
Cybercrime perspective

Since the release of commercial generative AI tools, we've seen phishing attacks surge by **1.265%**.

McKinsey
11/2024

- Statistic: Over 70% of advanced persistent threats (APTs) in 2024 already incorporated AI techniques
- Attackers will significantly automate phishing campaigns, zero-day exploitations, and malware coding by using AI. Emergence and application of multi-agent AI systems for good (e.g., cybersecurity co-pilots) and bad.
- There will be a democratization and commoditization of GenAI and ML related capabilities for offensive and defensive objectives
- AI-Regulation might lag behind due to fast evolving AI applications and geopolitical competition
- Data poisoning with deliberately injected false or corrupted data into an AI's may cause performance issues and inaccurate results

Impact on cyber insurance



- All risk owner & threat actors will be increasingly augmented with AI capabilities
- Democratization of TTP's will lower barriers for access to cybercrime scene
- Frequency of claims expected to rise
- Discussion about "Silent AI" will gather momentum

AI perspectives between hype, risks and advancement

Cybercrime perspective

	Highly capable state threat actors	Capable state actors, commercial companies selling to states, organised cyber crime groups	Less-skilled hackers-for-hire, opportunistic cyber criminals, hacktivists
Intent	High	High	Opportunistic
Capability	Highly skilled in AI and cyber, well resourced	Skilled in cyber, some resource constraints	Novice cyber skills, limited resource
Reconnaissance	Moderate uplift	Moderate uplift	Uplift
Social engineering, phishing, passwords	Uplift	Uplift	Significant uplift (from low base)
Tools (malware, exploits)	Realistic possibility of uplift	Minimal uplift	Moderate uplift (from low base)
Lateral movement	Minimal uplift	Minimal uplift	No uplift
Exfiltration	Uplift	Uplift	Uplift
Implications	Best placed to harness AI's potential in advanced cyber operations against networks, for example use in advanced malware generation.	Most capability uplift in reconnaissance, social engineering and exfiltration. Will proliferate AI-enabled tools to novice cyber actors.	Lower barrier to entry to effective and scalable access operations – increasing volume of successful compromise of devices and accounts.

Credit risk will probably rise in 2025 as cyber-attackers evade defenses with artificial intelligence and increasingly target large companies with the resources to pay high ransoms.

Moody's

- Besides big game hunting ransomware groups are more frequently targeting smaller businesses (revenue <\$20 million) rather than the resource-rich organizations (Securitymagazine)
- Estimated growth rates of 81% year-over-year increase from 2023 to 2024 (Securitymagazine) might prevail
- In 2024 the average downtime caused by ransomware increased to 16 days, up from 12 days in 2023
- The average attack has gotten more costly, with the average ransom payment more than doubling to almost \$4 million in 2024 (Sophos "The State of Ransomware 2024")
- 2024 saw the emergence or rebranding of 33 threat actors, contributing to a total of 5,477 leak site posts from 75 active groups (Rapid 7, "2024 Threat Landscape Statistics")

Impact on cyber insurance



- Ransomware will continue to be the largest risk & loss driver
- Tech progress and tactics point to a more complex and damaging ransomware landscape
- Current trend of increasing ransomware losses seems likely to continue in 2025

 Credit risk will probably rise in 2025 as cyber-attackers evade defenses with artificial intelligence and increasingly target large companies with the resources to pay high ransoms.

Moody's

- Further increasing frequency, automation and sophistication of ransomware attacks to expect. Especially AI will push scale, speed and precision
- Triple or layered extortion will remain mainstream with ransom for data decryption, theft of data and non-disclosure, and avoiding DDoS attacks
- Targeting critical vendor (including cloud service provider) and supply chains will shape systemic risk and cascading effects
- Unbroken trend of Cybercrime-as-a-Service with offerings ranging from platforms to subscription-based malware or AI enabled hacking tools will further lower the barriers to access ransomware business
- Harsh trend to use infostealer malware: Its simplicity, vast availability, and low costs made it a primary vector for ransomware or data breaches
- Ransomware will cost its victims approx. \$265bn annually by 2031 (Cybersecurity Ventures)

Impact on cyber insurance



- Ransomware is not a cybersecurity or insurance issue anymore – it has become a national or global security threat
- Little accumulation events like Change Healthcare or CDK might happen more often

Business email compromise (BEC) and Business Communication Compromise (BCC)



- The number of BEC detected by security firm Vipre in the second quarter 2024 was 20% higher than the same period in 2023. Two-fifths of them were generated by AI
- Social engineering scams will look more realistic than ever with the use of deepfakes
- LLM trained on a person's public posts can mimic speech, writing style, knowledge, and personality. Perfect impersonations will drive fraudulent activities and BEC/BCC
- BEC and “fake employee” scams need to be included in risk management operations

Impact on cyber insurance



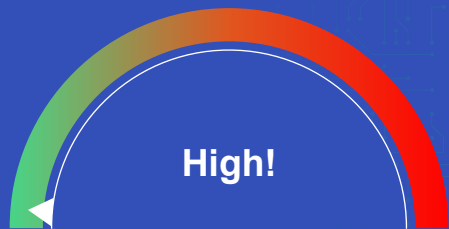
- High loss expectation in the field of BEC/BCC attacks with high dark figures
- Low sophistication actors might develop more easily in the future



Supply Chain

- The WEF indicated that 45% of organisations expect to face significant cyberattacks on their supply chains by 2025. 54% of large organizations highlight supply chain challenges as the greatest barrier to achieving cyber resilience
- With a 75% increase in cloud intrusions over the past year, securing the cloud is more critical than ever (CrowdStrike “2024 Global Threat Report”)
- Rise in cost of software supply chain attacks to businesses anticipated: \$138 billion by 2031, up from \$60 billion in 2025 (Cybercrime Magazine)
- The Orange Cyberdefense Security Navigator 2025 report stated that the U.S. is the epicenter of OT-targeted attacks, responsible for about 49 percent of all global incidents. Half of them aiming to seize control of industrial equipment
- Top 3 risks for organizations: Software compromise, Managed Service Provider compromise, single service disruption

Impact on cyber insurance

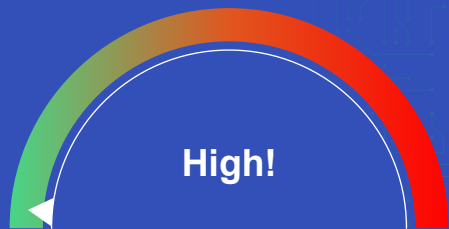


- Multiple loss scenarios possible: BI, CBI, data breach
- Digital bottlenecks and systemic risks will grow – e.g., cloud services, convergence between IT and OT...
- Difficult to assess 3rd party risk



- New US Administration will likely aim to limit federal government regulation of cybersecurity, with deregulation efforts attempting to balance national security concerns. Changes to certain agencies (e.g., CISA, DHS) are also likely
- Big Tech companies will be reducing controls around disinformation. Increasing intermingling between big tech and politics will have significant impact on regulation
- India's Digital Personal Data Protection Act, enacted in 2023, will likely go into effect in 2025
- Voices to ban ransom payments might get louder
- AI governance and regulation will dominate legislative agendas. Standards for AI will be available but remain a moving target

Impact on cyber insurance



- Rising liability for risk owner
- More regulation, compliance and reporting/breach disclosure requirements – e.g., NIS2, SEC, DORA...
- Data Breaches remain significant loss driver

Personal Lines

Trends & Developments



- 7.5bn people will be connected to the internet in 2030 (Cybersecurity Ventures)
- Social media platforms have become a cyber crime hot spot. AI-related scams, phishing, disinformation and the combination of social media and generative AI will enable even more harmful attacks. The big concern lies in how social media and GenAI are converging
- Criminals will exploit social media platforms not just to exfiltrate data and PII but also to craft highly targeted scams, impersonations, and fraud as well as to manipulate users into compromising corporate security
- Blurring lines between private and business life as well as legitimate communication and fraud (e.g., via professional networks like LinkedIn)
- More malicious QR-codes will trick users to click

Impact on PL cyber insurance



- Market penetration of personal lines still small, but there is a clear uptick
- Good loss ratios so far. Online fraud – especially when shopping/selling online is largest loss driver
- Blurring lines between private and professional life

Cyber Risk Management predictions

Main organizational challenges to cyber resilience that will remain beyond 2025

Small
organizations



Medium
organizations



Large
organizations



01

**Complex and evolving
threat landscape**

01

**Complex and evolving
threat landscape**

01

Third-party risk
management

02

Skills shortage

02

Third-party risk
management

02

**Complex and evolving
threat landscape**

03

Lack of incident response
preparedness

03

Complexity of environments
(e.g., IT, OT, IoT)

03

Complexity of environments
(e.g., IT, OT, IoT)

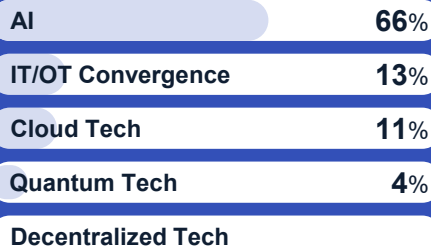
Cyber Risk Management predictions

Main organizational challenges to cyber resilience that will remain beyond 2025

Vendor assessment and compliance to all global regulation as **“Mission Impossible”**.

By 2029, **50 percent of organizations will use external attack surface scan data** to monitor their partners/suppliers in an effort to understand third-party risk. (IDC)

Top Cybersecurity Challenges



World Economic Forum:
Expectations from 409 CISOs & C-Level Execs from 57 countries, January 2025.

Despite AI and automation statistics indicate a widening cybersecurity gap with up to **4.8 million cybersecurity specialists missing**.

In 2025, we may see **clear progress in quantum computing technology**, shifting to quantum-resistant cryptographic algorithms.
The UN proclaimed 2025 as the “International Year of Quantum Science and Technology”.

- Softening tendencies and increasing competition in the original market might lead to rate decreases or coverage broadening (e.g., non-tech CBI, Tech E&O) as well as blended policies
- Financial restraints caused by economic situation may lead to a tendency of decreasing preparedness to spend money for (cyber) insurance
- Appropriate war exclusions are becoming more and more standard. Many markets seem to be fully committed (Europe, APA-regions). Mixed picture in the U.S.
- AI implementation and the use of GenAI will help in UW or Claim but AI-related threats will remain a major focus that impacts the frequency of losses
- Overall: primary insurers retain more business, original market is growing less than expected
- Increased Hiring of Cybersecurity Professionals by Cyber Insurance Companies



It appears that having some form of insurance aids organizations to become more cyber resilient:

Among organizations classed as highly resilient, only 7% claimed to not have cyber insurance.

World Economic Forum
“Global Cybersecurity Outlook 2025”



For your “personal outlook
2025 and beyond” **all the best!**