Allianz

Gen AI and evolving threats

- reshaping the insurance landscape

ALLIANZ COMMERCIAL

Overview

The convergence of artificial intelligence (AI) and cyber security is fundamentally transforming the risk landscape, presenting both unprecedented challenges and opportunities for the insurance industry. Our analysis reveals a dramatic surge in AI adoption across the cyber security sector, with enterprise implementation rates climbing from 49% to 69% year-on-year. One industry projection indicates cyber security AI spending will reach $46.3bn by 2027[1], while others indicate the total could be more than triple that amount in the following years. AI-enhanced threats have evolved in parallel: phishing attacks increasing 135% over a two month period[2], deepfake incidents increasing by 2000%[3], and AI-powered ransomware attacks achieving 67% higher success rates[4] in data exfiltration.

In response to this shifting threat landscape, the cyber insurance market shows strong growth potential, projected to expand from around US$14bn in 2023 to around $29bn by 2027[5]. According to McKinsey, AI could create $1.1trn in annual value for the insurance industry by 2030[6]. The insurance industry has witnessed a significant shift toward incorporating AI-specific risk coverage, with surveys often showing that 70%+ of providers are leveraging AI-driven risk assessment frameworks. These AI systems have revolutionized traditional approaches by analyzing real-time data from Internet of Things (IoT) devices, social media, and other sources, rather than relying solely on historical data and generalized statistics. This comprehensive approach has led to significant improvements in both operational efficiency and risk management capabilities, with insurers reporting reduced processing times and enhanced fraud detection through their AI implementations. For example, studies show a 43% improvement in early fraudulent claim detection alone[7].

As the digital risk landscape continues to evolve, the strategic integration of AI will become fundamental to providing effective risk management solutions and maintaining competitive advantage in the cyber insurance market. This transformation marks a crucial inflection point where the synergy between AI, cyber security, and insurance will define the future of risk protection in our increasingly interconnected digital ecosystem, making the ability to adapt and leverage AI technology paramount for insurers seeking to provide comprehensive protection against emerging cyber risks.

Introduction

In recent years, we've seen a big change in how computers and the internet work. This change is mainly the result of Generative AI (Gen AI), a new technology which can create text, images, and even computer code that look like they were made by humans. It's impressive, but it's also causing some problems.

As Gen AI develops, it's changing how cyber criminals attack computers and steal information. These new AI-powered attacks are harder to spot and stop. For example, AI can now create very realistic fake emails that trick people into giving away important information. It can also make fake videos and voice recordings that sound just like real people. This makes it easier for criminals to fool people and break into computer systems.

But it's not all bad news. The same AI technology is also being used to protect computers and networks. Many companies are now using AI to spot and stop cyber-attacks faster than ever before. In fact, more than two-thirds of businesses are now using AI for cyber security. This has created a race between the "good guys" and the "bad guys" in the world of cyber security.

All these changes are having a major impact on the insurance industry. Insurance companies are facing new challenges as they try to help protect their customers from these AI-powered cyber threats. They're creating new types of insurance to cover AI-related risks, and they're even using AI themselves to better understand these risks and identify insurance fraud.

The insurance industry is at a turning point. Companies that can keep up with these AI changes will thrive, while those that do not might struggle. As AI continues to change both how cyber-attacks happen and how we defend against them, insurance companies need to be ready to adapt quickly. In this report, we'll look closely at how AI is changing cyber security and the insurance industry, and what this means for the future.

1 Meticulous Research, Artificial Intelligence (AI) in Cybersecurity Market Worth $46.3 Billion by 2027- Market Size, Share, Forecasts, & Trends Analysis Report with COVID-19 Impact by Meticulous Research

2 Darktrace, How Phishing Attacks Are Becoming Harder to Identify, March 20, 2024

3 AI in Financial Fraud: Deepfake attacks soar by over 2000%, June 1, 2024

4 International Journal for Multidisciplinary Research, The Rise of AI-Powered Cybercrime: A Data-Driven Analysis of Emerging Threats, Poli Reddy Reddem

5 Munich Re, Global Cyber Risk and Insurance Survey 2024

6 McKinsey, Insurer of the future: Are Asian insurers keeping up with AI advances?, May 3, 2023

7 International Journal of Research in Computer Applications and Information Technology, The Transformative Impact Of AI On Insurance Underwriting: A Technical Analysis, Jan-Feb 2025

The evolving threat landscape

The world of cyber security is changing fast, mainly because of AI. As technology gets smarter, so do the people who want to use it to cause harm. Old cyber threats have become more dangerous and new risks have appeared. Understanding these changes is key to protecting ourselves and our businesses in the digital world.

Traditional vs. AI-enhanced cyber threats

Previously, cyber-attacks were simple and relatively straightforward. Like using a sledgehammer to break down a door, hackers would send out thousands of fake emails hoping someone would click on them. Today's AI-powered attacks are much smarter and sophisticated.

The evolution of AI has given rise to a new generation of sophisticated cyber threats that go far beyond traditional attack methods. These include deepfake technology that can perfectly mimic voices and videos for deception, AI-powered malware that actively evades detection while targeting valuable data, and intelligent social engineering systems that create convincing fake profiles by analyzing online behavior patterns. Additionally, AI has revolutionized traditional attack vectors like password cracking and distributed denial-of-service (DDoS) attacks by making them more precise and effective, with systems that can intelligently identify vulnerabilities and optimize attack timing for maximum impact.

Examples of AI-powered cyber-attacks

The audio deepfake scam: Criminals used AI to mimic a CEO's voice. They called a company manager and tricked him into transferring $243,000 to their account. The AI voice sounded so real that the manager didn't suspect anything.

Emotet's smart phishing: The Emotet malware used AI to create phishing emails that looked like they were part of existing email threads. This made people much more likely to open them and click on unsafe links.

The LinkedIn AI bot: This was used to create a fake profile to connect with thousands of people, including government officials, having the potential to gather sensitive information or spread misinformation.

Adaptive ransomware: Some new ransomware uses AI to learn the normal patterns of activity on a network. It then encrypts files and moves through the system in a way that looks like normal traffic, making it very hard to detect.

These examples show how AI is making cyber-attacks more sophisticated and harder to defend against. As AI continues to improve, we can expect to see even more advanced threats in the future. This is why it's crucial for cyber security defenses and insurance policies to keep evolving too.

Impact on the insurance industry

The advent of Gen AI and the rapidly evolving cyber threat landscape are profoundly transforming the insurance industry, bringing both opportunities and challenges in the future.

Transforming risk assessment and underwriting

- AI-powered data analysis enables more accurate risk profiling.
- Real-time risk assessment using the Internet of Things (IoT) and AI becomes possible.
- Predictive modeling for emerging AI-related risks can improve underwriting.

Policy coverage evolution: addressing AI-specific risks

- New types of insurance policies will be developed to cover liabilities arising from AI system errors or unexpected behaviors. e.g., autonomous vehicles or automated trading.
- Traditional cyber insurance is being expanded to explicitly cover AI-specific threats like deepfake attacks or AI-powered social engineering.
- As regulations around AI use evolve, insurers must ensure their AI-specific products comply with emerging legal frameworks.

Claims processing in the age of AI

- AI-powered automation streamlines claims handling.
- Machine learning enables faster and more accurate claims assessment.
- Ethical considerations in AI-driven claims decisions come to the forefront.

Enhancing fraud detection with AI

- Advanced pattern recognition significantly improves fraudulent claims identification.
- Natural language processing analyzes claim descriptions for inconsistencies.
- Balancing fraud detection with customer privacy and fair treatment becomes crucial.

Ethical considerations and potential biases

- Addressing potential biases in AI-driven underwriting and claims processing becomes a priority.
- Ensuring transparency and explaining ability in AI decision-making is essential.
- Maintaining human oversight of AI systems presents ongoing challenges.
- AI potentially helps identify and mitigate existing biases in insurance practices.
- Ethical use of AI in customer profiling and personalized pricing requires careful consideration.

Regulatory compliance and governance

- Insurers have to adapt to evolving regulations around AI use in insurance.
- New frameworks for AI governance within insurance organizations are being developed.
- Ensuring compliance across complex AI systems presents significant challenges.
- Regulatory technology (RegTech) solutions emerge to assist with AI-related compliance.
- International considerations for AI use in global insurance markets gain importance.

As the insurance industry navigates these challenges and opportunities, it must balance innovation with ethical considerations, customer trust, and regulatory compliance to successfully harness the power of AI in an increasingly digital and interconnected world.

Adapting insurance products and services

As the landscape of cyber threats evolves with the advancement of AI technologies, insurance companies must adapt their products and services to meet new challenges and customer needs. Insurers will need to develop next-generation cyber insurance policies, creating AI-specific coverages and exclusions, and offering innovative risk mitigation services and tools.

Next generation cyber insurance policies
The rapid evolution of cyber threats, particularly those powered by AI, necessitates a new approach to cyber insurance policies. Next-generation policies are being designed to address the complex and dynamic nature of modern cyber risks.

A shift towards continuous underwriting models that adjust coverage and premiums in real-time based on AI-driven risk assessments is anticipated. This could lead to more flexible, usage-based insurance products that better reflect the insured's actual risk profile. This dynamic approach represents a significant evolution from traditional annual policy reviews, allowing insurers to more accurately price risk while giving policyholders more control over their insurance costs through their security practices and risk management choices.

AI-specific coverages and exclusions
AI is likely to enable more granular, usage-based insurance products tailored to specific, short-term risks. This could open up new markets and make insurance more accessible to a broader range of customers. By leveraging AI's ability to process and analyze data in real-time, insurers can offer more flexible and personalized coverage options that better match customers' actual needs and risk profiles.

For example, an AI system might offer instant, short-term insurance coverage for valuable items based on real-time risk analysis of the item's location and usage. This dynamic approach could allow customers to pay only for the coverage they need, when they need it, while helping insurers better manage their risk exposure through more precise underwriting.

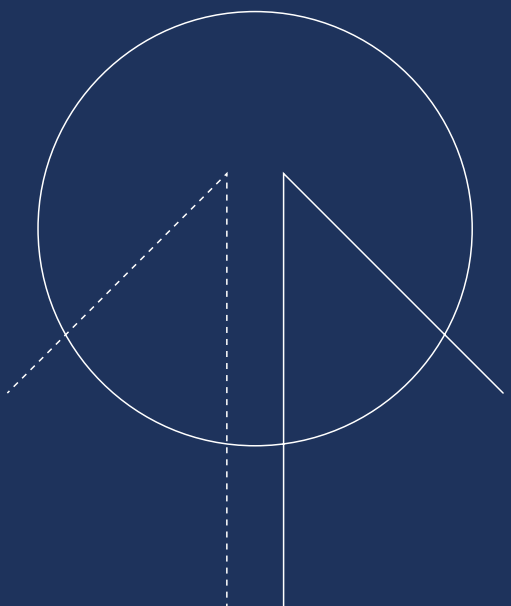
Risk mitigation services and tools
We expect the development of proactive insurance models that pre-emptively address potential risks identified by AI predictive analytics. This could shift the focus of insurance from reactive compensation to proactive risk mitigation. AI systems can analyze vast amounts of data to identify patterns and predict potential issues before they occur, enabling insurers to help prevent losses rather than just paying claims after the fact.

For example, an AI system might identify potential maintenance issues in industrial equipment and automatically arrange for preventive repairs, reducing the likelihood of a claim. This proactive approach not only minimizes business disruption but also helps reduce overall insurance costs through improved risk management.

By offering these adaptive insurance products and comprehensive risk mitigation services, insurers can position themselves as valuable partners in managing the complex risks associated with AI technologies. This approach not only helps protect clients from emerging threats but also fosters innovation by providing a safety net for organizations exploring cutting-edge AI applications.

Industry preparedness and response

Challenges ahead
The insurance industry's preparedness for AI-driven transformation and associated risks is a work in progress. While significant strides have been made in adopting AI technologies and developing new products, challenges remain in talent acquisition, legacy system modernization, and adapting to a complex regulatory environment. Collaborative efforts within the industry and with external partners are crucial for addressing these challenges effectively.



Collaborative efforts and information sharing

Recognizing the complex nature of AI-related risks, the insurance industry is increasingly focusing on collaborative efforts and information sharing, including:

- Industry consortiums.
- Public-private partnerships.
- Information sharing platforms.
- Cross-industry collaboration.
- Academic partnerships.
- Open-source initiatives.

Regulatory landscape and compliance challenges

The regulatory environment surrounding AI in insurance is complex and rapidly evolving, presenting significant compliance challenges for the industry. Factors to consider include:

- Emerging AI regulations.
- Data protection and privacy.
- Algorithmic fairness and non-discrimination.
- Model risk management.
- Cross-border considerations.
- Ethical AI guidelines.
- RegTech.
- Cyber security regulations.

The future of insurance in an AI-driven world presents both significant challenges and opportunities. Insurers that proactively adapt to AI-enhanced cyber threats, evolve their business models, invest in talent and partnerships, and prioritize ethical AI practices will be best positioned to thrive. By embracing AI as a transformative force while maintaining a strong focus on risk management and ethical considerations, the insurance industry can enhance its ability to protect individuals and businesses in an increasingly complex and interconnected world.

Allianz Commercial:

Rajat Dubey
Senior Cyber Risk Consultant
rajat.dubey1@agcs.allianz.com

Rishi Baviskar
Global Head of Cyber Risk Consulting
rishi.baviskar@allianz.com

For more information contact
az.commercial.communications@allianz.com

Follow Allianz Commercial on LinkedIn

www.commercial.allianz.com

Allianz Global Corporate & Specialty SE, Königinstraße 28, 80802 Munich, Germany.
Commercial Register: Munich, HRB 208312

February 2025