cowbell®

Innovations in Artificial Intelligence and Machine Learning

Examining AI and ML's Impact on Cybersecurity and Cyber Insurance in the Year Ahead

Q4 Quarterly Report 2023

Highlights & Contents

Introduction

On November 30, 2022, OpenAI released a public version of ChatGPT and within two months, attracted over one hundred million users. For many, this experience was their first interaction with AI as more broadly, society began to understand the enormity of this transformative technology. That was the start of a corporate "arms race," with Big Tech and VCs investing billions of dollars in generative AI startups and the largest tech news story of the year.

In reality, many enterprises have been leveraging AI to improve operational efficiency for the last several years and importantly, the emergence of enhanced AI models has also advanced cyber insurance risk modeling and threat detection, allowing insurance companies to construct more accurate cyber risk profiles. While numerous improvements are associated with AI, from automation to enhanced customer service, this historic leap towards an AI-driven future can come at a cost, as AI and machine learning (ML) innovations introduce more advanced cyber threats.

In this report, we explore the improvement and potential threats associated with the innovation of artificial intelligence and machine learning, and discuss its growing impact on cybersecurity and cyber insurance.

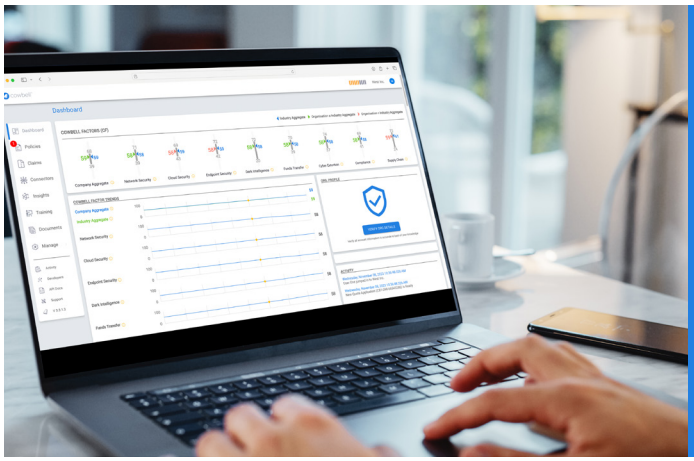
Artificial Intelligence's Potential Influence on Cyber Threats

The strategic implementation of AI technologies can empower organizations to scale their operations and improve efficiency. From data analysis, to hyper personalization, to market segmentation, AI enhances an organizations' ability to capitalize on new business opportunities. AI-driven systems can also automate threat detection, response, and mitigation processes, providing a proactive defense against evolving cyber threats.

However, the same capabilities that make AI a powerful ally in cybersecurity also poses risks:

- **Rapid developments in AI and ML** will increase the frequency of cyber threats, through techniques such as automated phishing, presenting an increased risk for small and medium-sized enterprises (SMEs).
- **Cyber vulnerabilities** can be more easily exploited as cybercriminals can leverage AI to design and deploy malware that is capable of learning and adapting, making it more challenging to detect and mitigate using traditional cybersecurity measures.
- **AI-generated deepfake content** can lead to identity theft and fraudulent activities. This poses a threat to the trustworthiness of digital communication and can have serious consequences for both individuals and organizations.
- **AI can analyze vast amounts of data** to craft sophisticated social engineering attacks, tailoring messages to exploit specific individuals or groups. This targeted approach increases the effectiveness of social engineering tactics.
- **The integration of vast quantities** of third-party data into systems increases the amount of vulnerabilities and potential penetration points.

As AI continues to advance, the cybersecurity landscape must evolve to harness its benefits while effectively mitigating the risks associated with malicious AI applications. Collaboration between the cybersecurity community, researchers, and industry stakeholders is critical to stay ahead of evolving risks and maintain trust. We are more secure when we work together as a part of a broader ecosystem.



"Cowbell is leading the way in our usage of AI for the betterment of cyber insurance. We continue to use AI and ML to analyze vast amounts of data to identify patterns and anomalies, helping SMEs detect and respond to security threats in real-time."

Rajeev Gupta
Co-Founder & CPO

Artificial Intelligence and Machine Learning's Impact on the Cyber Insurance Market

The emergence of a more robust AI system will provide an advanced methodology for determining a cyber environment's security risks, improving the cyber insurance risk market. Insurers are increasingly leveraging AI and ML to assess and mitigate risks more effectively. These technologies enable insurers to analyze vast amounts of data to identify patterns, detect anomalies, and assess the cybersecurity posture of potential policyholders.

This data-driven approach allows for more accurate underwriting, enabling insurers to tailor policies based on an organization's specific risk profile. Furthermore, AI and ML contribute to the development of predictive models that can forecast emerging cyber threats, helping insurers stay ahead of evolving risks.

> **"Companies continue to rely on technology in the underwriting process. We will be launching a new product in 2024 that has even more AI capabilities than ever before."**
>
> **Caroline Thompson**
> Chief Underwriting Officer

On the claims side, these technologies facilitate faster and more precise claims processing by automating the assessment of damage, validating claims, and identifying potential fraud.

Simultaneously, increased reliance on AI will pose new threats for organizations and companies will need to continuously monitor and adapt their offerings to protect and serve customers.

Cowbell's Approach

At Cowbell, we harness technology and data to provide small and medium-sized enterprises with advanced warning of cyber risk exposures and customized coverage adaptable to today's and tomorrow's threats.

Most importantly, we are continuously improving. With four years of (re)learning and trillions of data points, we updated our risk model and evolved our approach to risk assessment. We replaced pre-modeled proxy data with unprocessed raw data, giving us more control and precision; significantly improved predictive accuracy by using Cowbell's own claims data; added granularity to NAICS codes and classification; enhanced our ability to reprioritize vulnerabilities; and incorporated a new data source to evaluate 3rd party vendor risk.

The substantial volume and improved quality of data, coupled with a more robust closed-loop system and refined labeling and classification, has significantly influenced the effectiveness of our Cowbell Factors, our recently patented proprietary technology. The enhancements have resulted in a 436% improvement in predicting claims frequency and a 254% increase in predicting claims severity. You can read more about how Cowbell Factors is redefining cyber risk quantification here.

Executive Leader 2024 Predictions

As AI continues to take center stage, the inherent risks will continue to grow exponentially. Experts from every sector are considering the implications and considering how to best mitigate threats.

According to a recent attorney analysis from WestLaw, "A.I.-related claims can take many forms, including, for example, alleged violations of employment law, breaches of data privacy statutes, breaches of fiduciary duties or professional obligations, violations of securities laws, intellectual property infringement, or any other number of events, acts or omissions." These risks are critical for companies to consider when purchasing coverage.

Computer scientists from the National Institute of Standards and Technology (NIST) recently warned of the dangers when AI systems malfunction as a result of exposure to untrustworthy data. Attackers are taking advantage of this vulnerability and they identified four major types of attacks including: evasion, poisoning, privacy and abuse attacks.

Our leadership team understands that the emergence of AI and generative AI means we have to do more for our policyholders and work together as an industry to mitigate future risks. Looking to 2024, we are committed to ensuring our adaptive coverage options meet the needs of small and medium-sized enterprises (SMEs).

> **"Cyber products need to evolve as technology and innovation evolve. This will — to some capacity — include AI-specific coverages as well as value-added services."**
>
> **Jack Kudale**
> Founder & CEO

cowbell®

Resources

As always, we are committed to partnership and we are here throughout every step of the journey – not just when it's time to pay a claim. We believe that the best defense is offense and we provide our partners and policyholders the tools and resources they need to successfully manage their risk. Some examples are listed below –

- Cowbell Academy, courses to help you better understand trends, threats, and managing risks.
- Cowbell Rx, access to our trusted network of vetted partners to manage your risk and exposures.
- Podcasts and Webinars, learning tools to help you upskill.
- Cowbell Data and Insights, our blog that features advice and insights from our experts.

Adaptive Cyber Insurance

support@cowbellcyber.ai

(833) 633-8666

cowbell.insure

US0011 0124