S&P 500’s AI adoption may invite data breaches, new research shows

VILNIUS, LITHUANIA, July 31, 2025 /EINPresswire.com/ -- Artificial intelligence is now part of business operations in many S&P 500 companies. However, Cybernews researchers have identified hundreds of potential issues ranging from insecure AI output to critical infrastructure attack vectors across sectors such as infrastructure, finance, and healthcare.

Researcers has identified 327 S&P 500 companies that publicly report using AI tools in their operations and analyzed how these organizations deploy AI in daily business activities. Investigation tracked a wide range of use cases, from language model-powered analytics and internal business tools to customer-facing integrations and automated support systems.

The result is a look at just how deeply AI is woven into the daily workflows of America’s corporate giants – and the mounting security risks that come with this transformation.

Bad output, data leaks, and IP theft: the big three

The research spotlights three dominant potential threat vectors.

First, insecure output is the most widespread AI risk across the S&P 500, with 205 potential issues that could cause an incident largely spanning technology, finance, and healthcare. Chatbots could be leaking customer data, finance bots giving bad investment advice, or a medical AI hallucinating treatments that are unsafe or not fully tested yet.

Next comes data leakage with 146 potential threats. This is when AI models accidentally spill sensitive information: customer PII, business financials, even proprietary source code. It often happens through prompt injection, where attackers craft clever queries to extract training data or past chat logs. Sometimes, it’s just the model “remembering” things it shouldn’t.

Intellectual property theft rounds out the top three, with 119 cases of proprietary business data or R&D secrets being potentially exposed or stolen via AI systems. Attackers use model extraction techniques – think of it as digital industrial espionage. By bombarding an exposed AI model with thousands of queries, hackers can reverse-engineer its logic, recreate its capabilities, and siphon off the very data and trade secrets that make your business unique. Sometimes, insiders or compromised APIs can make the job even easier.

The rapid growth of AI in business is not only transforming how companies operate but also reshaping the threat landscape. According to Žilvinas Girėnas, head of product at nexos.ai, the biggest risks for enterprise AI today are less about the technology itself and more about how it's being used, secured, and trusted.

"Insecure AI outputs, data leaks, and IP theft are the new primary risks for every industry using AI, from finance to healthcare to critical infrastructure," Girėnas said.

"It's not enough to deploy AI and hope for the best. Businesses need to develop AI with the same safety standards as airplanes: constant oversight, clear guardrails, and a zero-trust approach. Every AI decision must be considered potentially wrong until proven correct, and every input must be monitored to prevent sensitive data from leaking or trade secrets from escaping."

He also noted that as AI adoption increases, new risks such as model manipulation, supply chain attacks, and systemic bias are quickly emerging threats that require equal attention.

Other risks are gaining ground fast

The algorithmic bias risk has been documented 37 times. It happens when the model is trained using data that doesn't match current societal norms.

Our research also found 49 documented cases of possible critical infrastructure attack vectors where AI vulnerabilities could be weaponized against the systems that keep society running: power grids, water treatment plants, factories, and more. The energy sector alone has 35 potential issues, making it the top target for these high-stakes exploits.

Supply chain disruptions (54 instances), model evasion (38), and data poisoning (24) are also on the rise, showing that the attack surface is both broad and evolving.

Sensitive sectors, real consequences

What's most dangerous is where AI vulnerabilities are showing up – and which sectors are hit hardest. While healthcare, energy, and finance remain high-profile targets, the data reveals that technology, industrial, and retail sectors are just as exposed, if not more so, to a wide spectrum of AI-driven risks.

Technology software and semiconductors top the list, with 202 total potential issues across 61 companies. This sector alone reported 40 cases of IP theft, 34 instances of insecure output, and 32 of data leakage.

Financial services and insurance (158 total potential issues, 56 companies) face the highest number of potential data leakage issues (35), and a striking 22 cases of algorithmic bias, highlighting the dual threats of sensitive customer information exposure and systemic discrimination in lending or credit scoring. The sector also contends with 32 potentially insecure output instances and 18 cases of potential model evasion, where attackers could attempt to bypass fraud detection systems.

Healthcare and pharmaceuticals (149 potential risks, 44 companies) are particularly at risk for patient safety, with 19 identified potential issues, as well as 24 data leak risks and 28 insecure output risks.

Industrial and manufacturing (114 potential issues, 41 companies) and critical infrastructure and energy (103 potential issues, 37 companies) together account for 38 critical infrastructure attack vectors and 12 potential supply chain disruptions.

Retail and consumer goods (92 potential issues, 36 companies) and logistics and transportation (32 potential issues, 10 companies) are increasingly reliant on AI for inventory management, personalized marketing, and route optimization. With 20 and 2 data leakage risks, respectively, and a combined 28 potential supply chain disruptions, these sectors face mounting threats to both customer privacy and operational continuity.

Even defense and aerospace (36 potential issues, 9 companies) and media and entertainment (25 potential issues, 9 companies) are not immune, reporting notable counts of IP theft, insecure output, and national security risks. In defense, 8 potential national security risk issues reveal the potential for AI vulnerabilities to escalate beyond corporate losses to matters of state.

“In each of these sectors, the result of AI integration is a paradox: unprecedented efficiency gains exist alongside systemic fragility, where a single compromised model could trigger cascading failures across energy grids, financial markets, or healthcare systems. This tension between innovation and vulnerability defines corporate America’s AI moment,” said Martynas Vareikis, Security Researcher at Cybernews.

Ruta Pauliukonyte
Cybernews
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/835780205

in today's world. Please see our Editorial Guidelines for more information.