Corporate race to use AI puts public at risk, study finds

February 26 2024, by Julie Schomberg

Credit: Pixabay/CC0 Public Domain

A rush by Australian companies to use generative Artificial Intelligence (AI) is escalating the privacy and security risks to the public as well as to staff, customers and stakeholders, according to a new study.

The University of the Sunshine Coast research, published in a paper in

AI and Ethics, warns that rapid AI take-up is leaving companies open to wide-ranging consequences.

These include mass data breaches that expose third-party information, and business failures based on manipulated or "poisoned" AI modeling—whether accidental or deliberate.

The study included a five-point checklist for businesses to ethically implement AI solutions.

UniSC Lecturer in Cyber Security Dr. Declan Humphreys said the corporate race to adopt generative AI solutions like ChatGPT, Microsoft's Bard or Google's Gemini was fraught with not just technical, but moral issues.

Generative AI applications turn large amounts of real-world data into content that appears to be created by humans. ChatGPT is an example of a language-based AI application.

"The research shows it's not just tech firms rushing to integrate the AI into their everyday work—there are call centers, supply chain operators, investment funds, companies in sales, new product development and human resource management," Dr. Humphreys said.

"While there is a lot of talk around the threat of AI for jobs, or the risk of bias, few companies are considering the cyber security risks.

"Organizations caught in the hype can leave themselves vulnerable by either over-relying on or over-trusting AI systems."

The paper was co-authored by UniSC experts in cyber security, computer science and AI, including Dr. Dennis Desmond, Dr. Abigail Koay and Dr. Erica Mealy.

It found that many companies were making their own AI models or using third-party providers without considering the potential for hacking.

"Hacking could involve accessing user data, which is put into the models, or even changing how the model responds to questions or the answers it gives," Dr. Humphreys said. "This could mean data leaks, or otherwise negatively affect business decisions."

He said legislation had not kept pace with issues of data protection and generative AI. "This study recommends how organizations can ethically implement AI solutions by taking into consideration the cyber security risks."

The five-point checklist includes:

- Secure and ethical AI model design
- Trusted and fair data collection process
- Secure data storage
- Ethical AI model retraining and maintenance
- Upskilling, training and managing staff.

Dr. Humphreys said privacy and security should be a top priority for businesses implementing artificial intelligence systems in 2024 and beyond.

"The rapid adoption of generative AI seems to be moving faster than the industry's understanding of the technology and its inherent ethical and cyber security risks," he said. "A major risk is its adoption by workers without guidance or understanding of how various generative AI tools are produced or managed, or of the risks they pose.

"Companies will need to introduce new forms of governance and regulatory frameworks to protect workers, sensitive information and the

public."

More information: Declan Humphreys et al, AI hype as a cyber security risk: the moral responsibility of implementing generative AI in business, *AI and Ethics* (2024). DOI: 10.1007/s43681-024-00443-4

Provided by University of the Sunshine Coast