Gustav d'Assonville

Senior Manager
Technology Assurance: Cyber
Tel: +27 66 304 2062
Email: gustav.dassonville@kpmg.co.za

Managing and mitigating third-party cyber risks with the use of artificial intelligence

Introduction

Modern interconnected digital landscapes mean that organisations face unprecedented cybersecurity challenges. The growing complexity of these ecosystems render traditional defence mechanisms insufficient to mitigate ever-evolving threats. Cybersecurity vendors are leveraging these integrated technologies to build more advanced product iterations and increase the efficiency and efficacy of their defensive toolsets.

At the same time, artificial intelligence (AI) is emerging as a driving force behind the next digital revolution. Generative AI in particular, long restricted to primitive chatbots, has grown into complex systems such as ChatGPT-4 and Gemini Pro, redefining the possibilities around how insurers can engage with customers, analyse and process claims, create and underwrite policies and manage risk.

However, as with any technological advancement, AI has its own set of challenges, including data privacy, accountability and AI hallucination[1]. The concept of "Trusted AI" has emerged as a set of guiding principles that ensure AI systems are safe, accountable and transparent. AI has shown promise in helping organisations tackle one of the more challenging aspects of cyber risk management: third-party cyber risk management (TPCRM). While it is no panacea, under the right use cases and supported by responsible governance, AI can unlock incredible benefits.

The rapid development of AI

In the second quarter of 2024, OpenAI and Google released their most advanced iterations of their respective Large Language Models (LLM) AI platforms, amongst a litany of new AI startups. Both excel in producing content that may be considered "human like", and both provide improved language comprehension from text. Digital personal assistants are now equally capable of reviewing software source code on screen while having spoken discussions in real time with low latency, including real-time translation. AI integration across multiple product lines creates ease of access and reduces user friction. In the insurance industry, LLMs are already being used to analyse reports, claims and regulatory documents, the organisation and screening of client documents and policy compliance analysis.

[1] AI hallucinations are incorrect or misleading results that AI models generate. These errors can be caused by a variety of factors, including insufficient training data, incorrect assumptions made by the model, or biases in the data used to train the model. (https://cloud.google.com/discover/what-are-ai-hallucinations)

While these developments demonstrate real benefits to users, threat actors[2] are also leveraging these breakthroughs to modernise their own attack vectors and introduce innovative strategies to compromise people, processes and technologies. As the saying goes "seeing is believing", threat actors can now utilise AI to create deep fake audio and video to create social engineering attacks so realistic it would seem like science fiction. Unfortunately, this is the reality faced by many cybersecurity teams that are finding it increasingly difficult to outpace threat actors. Responsible AI usage can go a long way towards alleviating the challenges.

Importance of TPCRM

TPCRM has grown into a significant area of challenge for organisations in recent years, given the complex and fast-paced eco-systems in which it operates, with many organisations being heavily dependent on a significant number of third parties for a vast array of operational processes.

In a recent filing, a large US-based insurer notified the public, its policyholders and other key stakeholders of a significant data breach incident that occurred. The breach, which affected more than 28 000 people, was directly attributable to a weakness in a third-party service provider's software. The information acquired ranged from an individual's financial account number to credit/debit card number (in combination with the security code, access code, password or PIN for the account). This is but one in a plethora of examples of such breaches.

Industry regulators are not turning a blind eye. Following on the heels of the Protection of Personal Information Act (POPIA) and the Cybercrimes Act, the Financial Sector Conduct Authority (FSCA) and the Prudential Authority (PA) in May 2024 released the Joint Standard on Cybersecurity and Cyber Resilience, with TPCRM being a significant focus point for the standard.

On the AI front, government and industry stakeholders in South Africa recently convened a National AI Summit to share the contents of a draft National AI Plan. Further afield, the European Union (EU) published the ground-breaking Artificial Intelligence Act (EU AI Act) during August 2024. The AI Act is expected to set a new global standard for AI regulation, targeting compliance by 2026.

Leveraging trusted AI for third-party cyber risk management

AI is increasingly being used to perform dynamic risk assessments on third-party cybersecurity postures. This involves leveraging machine learning models to assess third-party risk likelihood and impact, and utilising correlation analysis to incorporate internal and external data sources more efficiently than even before. Other demonstratable use cases include inspecting control evidence submitted as part of due diligence during the TPCRM lifecycle, by leveraging LLM's trained on leading security practices.

To stay ahead, third-party risk service offerings have innovated with the integration of AI, machine learning (ML) and natural language processing (NLP) into TPCRM solutions. Use cases of AI-enabled digital workers (e.g. AI trained chatbots) across the TPCRM lifecycle provide increased visibility, better efficiencies, reduced operating costs and informed decision making for better risk management.

Early information coming out of KACEY (KPMG's Intelligent Automation capability framework for transforming third-party risk management programs) provides interesting statistics, with some successful implementation results indicating a multiple factor increase in program efficiency while reducing costs by more than 50%.

[2] Threat actors, also known as cyberthreat actors or malicious actors, are individuals or groups that intentionally cause harm to digital devices or systems. Threat actors exploit vulnerabilities in computer systems, networks and software to perpetuate various cyberattacks, including phishing, ransomware and malware attacks. (https://www.ibm.com/topics/threat-actor)

The effective use of trusted AI solutions allows security teams to concentrate on strategic tasks, reducing the leg-work associated with onerous manual tasks. As organisations become ever more connected, the strategic deployment of trusted AI solutions offers a promising path forward, including, but not limited to:

- Increased capacity to assess the rapidly increasing volume of third-party usage;
- Consistent and reliable risk information;
- Alignment for communicating and understanding third-party risk across functions and measuring program performance over time;
- Breaking down information silos preventing a co-ordinated approach throughout organisations, and lead to better utilisation of third-party data; and
- Detecting and responding to risk posture changes in real time with dynamic ongoing assessment processes.

Conclusion

The impact of AI is vast and not yet fully appreciated. One thing is certain: it cannot be ignored. As organisational environments evolve with advancements in technology, so do the potential threats. The integration of AI in TPCRM processes opens new avenues for improving efficiency and quality in risk management. AI will assist forward thinking organisations to better navigate third-party risks, thereby safeguarding their operations and maintaining resilience against evolving threats. Organisations that are considering the integration of AI into their architecture, should create, build and execute a strategy and framework for deploying AI technologies responsibly and ethically, with demonstrable return on investment.

References

https://assets.kpmg.com/content/dam/kpmg/za/pdf/KPMG%20SOUTH%20AFRICA%20CEO%20OUTLOOK%202023.pdf

https://assets.kpmg.com/content/dam/kpmg/za/pdf/2023/6.%20Generative%20artificial%20intelligence%20(AI)%20in%20the%20insurance%20sector-%20a%20revolution%20in%20the%20making.pdf

https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2024/third-party-security-in-2030.pdf

https://www.insurancebusinessmag.com/us/guides/the-insurance-industry-cyber-crime-report-recent-attacks-on-insurance-businesses-448429.aspx

https://www.dcdt.gov.za/topics/495-national-ai-summit.html

https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf