AIB REVIEW
BY THE AUSTRALIAN INSTITUTE OF BUSINESS

AUSTRALIAN INSTITUTE of BUSINESS

Generative Artificial Intelligence Reshaping Business: Adapting Cybersecurity Strategies for the New Era

Vasiliki Vaso Charitsis, Senior Communications Consultant, Mackenzie Health, and member of the Australian Institute of Business (AIB) Alumni Industry Panel (Marketing & Entrepreneurship).
Sallina Jeffrey, CEO and Founder, The Mentoring Movement (TMM), and member of the Australian Institute of Business (AIB) Alumni Industry Panel (Marketing & Entrepreneurship).
Aliye Ozcan, Program Director, IBM Consulting Hybrid Cloud Service Global, and member of the Australian Institute of Business (AIB) Alumni Industry Panel (Marketing & Entrepreneurship).
Arthur Sitaramayya, Senior Business and Delivery Leader – IBM Consulting, Hybrid Cloud Management, APAC and member of the Australian Institute of Business (AIB) Alumni Industry Panel (Marketing & Entrepreneurship).

AIB Review, Issue 11

Introduction

In today's digital age, where data is vital to the existence of businesses and cyber threats loom large, safeguarding against attacks has never been more critical. The harmonious integration of generative artificial intelligence (GenAI) into business practices and policies demands a proactive approach, a discerning mindset to anticipate threats and an innovative business culture to seize opportunities. Failing to grasp the nuances of GenAI's influence on cybersecurity could render businesses vulnerable to risks, erode consumer trust and impede growth.

This article provides a discerning lens through which organisations can dissect the multifaceted nature of GenAI by shining a light both on its darker dimension and innovative potential. The objective of the article is to help readers understand essential facets of GenAI and its impact on cybersecurity. GenAI is not to be feared but viewed as a transformative platform that can be leveraged in this rapidly evolving technological landscape.

What is Generative Artificial Intelligence (GenAI)?

GenAI is a subset of deep learning systems capable of autonomously generating content, insight, or solutions across various data formats, including text, images and videos. GenAI can empower organisations to drive innovation, streamline operations and reduce costs by automating design processes, content creation and scenario simulations. Additionally, it can help organisations maintain agility and resilience, differentiate themselves from their competitors and provide a competitive advantage. As GenAI steadily integrates into industries from finance and pharmaceuticals to entertainment and retail, its transformative potential becomes increasingly evident. However, with this type of growth, there is an urgent need to re-evaluate cybersecurity paradigms due to its ability to create deep-fakes and deceptive data.

Why is this Important, and Why Now? A Cybersecurity Viewpoint

The integration of GenAI into business practices has the potential to reshape cybersecurity strategies. Firstly, GenAI can actively monitor network traffic and swiftly identify anomalies. This capability can improve incident detection and response times, allowing organisations to protect their systems and safeguard their data. Secondly, GenAI excels in analysing large amounts of data and identifying patterns that may signify a potential cyber threat. This analytical ability equips organisations with a deeper understanding of the types of attacks likely to target their systems, facilitating the development of more effective security measures.

Lastly, GenAI can automate routine cybersecurity tasks, including patch management and vulnerability assessments. By automating these types of tasks, organisations can concentrate on more complex tasks and enable faster response times to emerging threats. The integration of GenAI into business practices holds the promise of fostering more effective and efficient cybersecurity strategies that could result in strengthening an organisation's ability to better protect its systems and data from cyber threats.

Threats

While GenAI has the potential to bolster cybersecurity efforts, it also introduces a host of challenges and threats. A major concern is the emergence of adversarial attacks, wherein GenAI algorithms can be manipulated to produce erroneous predictions or classifications. In cybersecurity, hostile attacks can be used to deceive security measures or evade detection, allowing malicious actors to bypass defences, posing a threat to digital security.

Moreover, the issue of bias and discrimination is just as critical. GenAI algorithms are reflections of the data they are trained on. When data contains biases, the GenAI algorithm may exacerbate these biases, which can manifest in various domains and end processes, to potentially overlook certain cybersecurity threats. Subsequently, in the pursuit of fortifying defences against cyber threats or attacks, GenAI relies on vast datasets. However, this dependence on data raises concerns about data privacy. Given that GenAI requires access to large amounts of data, organisations must be vigilant against the risks associated with exposing sensitive information. Thus, organisations must mandate the development of robust architectural frameworks, prioritising data privacy and security.

Further, the complexity of GenAI can obscure the rationale behind decisions and predictions, making it difficult to identify potential vulnerabilities or manipulative actions. This underscores the importance of establishing corporate governance structures and implementing transparent measures. Equally important, as GenAI continues to advance in sophistication, the prospect of malicious actors harnessing the power of this type of technology for cyber-attacks becomes increasingly imminent. For instance, imagine GenAI being used to craft convincing phishing emails or orchestrate automated assaults on vulnerable business systems. Thus, the above-mentioned points demonstrate the critical importance of not only fortifying cybersecurity defences but also anticipating and mitigating the possible threats that GenAI poses.

Opportunities

Nevertheless, GenAI presents many promising opportunities for cybersecurity, each offering advantages that can help an organisation protect their digital assets and data. One such opportunity

lies in improved threat detection. GenAI can analyse large amounts of data, uncovering subtle patterns and potential threats that often elude the notice of traditional security tools. Consider the scenario where an organisation's network traffic undergoes a slight yet suspicious change that could signify an impending cyber-attack. GenAI, with its analytical effectiveness, detects this anomaly, enabling the organisation to promptly and effectively respond, thwarting a potential breach.

Subsequently, in vulnerability management, GenAI can help organisations prioritise vulnerabilities based on their potential impact, assisting organisations in allocating resources efficiently and reducing the risk of cyber-attacks. Beyond detection, GenAI can be leveraged for better decision-making by providing insights and recommendations. For instance, GenAI can be used to analyse historical data to inform security policy adjustments and advise on optimal responses to emerging threats, thus helping organisations navigate the evolving and complex landscape of cyber risks more effectively and efficiently.

Additionally, scalability is another domain where GenAI can automate many cybersecurity tasks, allowing organisations to scale their cybersecurity efforts more effectively as their business grows. Given GenAI's ability to automate cybersecurity tasks and streamline processes, organisations can scale their cybersecurity efforts seamlessly. For those responsible for cybersecurity efforts, it is noteworthy that this adaptability ensures that organisational security measures remain robust and effective, regardless of the size or pace of the organisation's growth.

Lastly, one of the most compelling opportunities for organisations to leverage GenAI is the chance to enhance customer trust. By implementing cybersecurity measures that leverage GenAI, organisations can proactively protect customer data, bolstering their reputation and fostering trust and confidence among customers in today's data-sensitive digital landscape.

Recommendations

To leverage GenAI in the battle against cyber-attacks, organisations can take the following proactive steps:

- Identify strategic integration points: Identify areas within the organisation's cybersecurity framework where GenAI can improve cybersecurity, including incident detection and response, threat intelligence, vulnerability management and identity and access management.
- Craft and deploy a clear integration strategy: Develop a clear strategy for integrating GenAI into existing cybersecurity frameworks, including identifying the specific use cases for GenAI, determining data sources that will be used to train the GenAI models, and defining the metrics to measure success.
- Embrace learning and adaptation: Ensure GenAI models used for cybersecurity are regularly updated and retrained to reflect changes in the threat landscape and to address potential biases or errors in the models.
- Implement governance and accountability: Implement proper governance and oversight to ensure GenAI for cybersecurity is transparent and accountable, including establishing policies and procedures for the use of AI, ensuring data privacy and security are maintained, and conducting regular audits and assessments to ensure compliance with relevant regulations.

- Invest in infrastructure and talent: Recognise that successful deployment of GenAI demands investment, including investing in high-performance computing resources, data scientists and cybersecurity experts trained in the use of AI.

Conclusion

In conclusion, in today's digital age, where data is invaluable and cyber threats continue to evolve, leveraging GenAI is no longer a choice but a strategic necessity. The dual nature of GenAI - with its promise of enhancing cybersecurity while introducing new challenges - highlights the need for a proactive approach. To succeed, organisations must leverage GenAI, establish governance and accountability frameworks, and invest in the necessary infrastructure and talent to safeguard digital assets and customer trust. By doing so, organisations will fortify their cybersecurity defences and stay ahead in the evolving digital landscape. Embracing and leveraging GenAI is no longer optional - it is what will separate leaders from followers.

Vasiliki Vaso Charitsis

Senior Communications Consultant, Mackenzie Health

Vasiliki Vaso Charitsis is a Senior Communications Consultant with over 15 years of experience in strategic communications and marketing. She holds an MBA and a Bachelor of Business Administration (BBA), along with a Master's Certificate in Marketing & Communications Leadership, and a professional certificate in Communications & Public Relations. Vasiliki currently serves at Mackenzie Health, accentuating the impact of the organisation's two-hospital model of care, and enhancing its digital healthcare brand. Her career includes roles at Desjardins, Surrey Place and Special Olympics Canada, showcasing her expertise in public relations, crisis management and supporting diverse communities.

Sallina Jeffrey

CEO and Founder The Mentoring Movement (TMM)

Sallina Jeffrey is a prominent entrepreneur and CEO of The Mentoring Movement Pty Ltd (TMM), specialising in organisational transformation and technology solutions. She excels in deploying scalable mentoring software, enhancing employee engagement within 24 hours. With an MBA, Sallina blends academic knowledge and practical experience, focusing on decreasing employee disengagement. A thought leader in artificial intelligence, she also serves as TMM's Advisory Board Chair, mentors MBA candidates, and has a technology, media and marketing background. Her expertise includes digital media, AI, change management and corporate governance. Sallina aims to revolutionise workplace dynamics and mentorship, promoting happier, more engaged work environments.

AIB REVIEW
BY THE AUSTRALIAN INSTITUTE OF BUSINESS

Aliye Ozcan

Program Director, IBM Consulting Hybrid Cloud Services

Aliye Ozcan is a Program Director at IBM Consulting Hybrid Cloud Services leading Marketing and Communications globally. With over 30 years of experience in the IT industry, her expertise spans information governance and data management, AI strategy, hybrid cloud, product development and marketing. Aliye is adept in audience-centric messaging and customer-advocacy storytelling, leveraging her deep understanding of Hybrid Cloud, Data and AI. She has held various leadership roles in IBM's Data and AI Technology Marketing, including DataOps, Data Governance and Strategy. Additionally, Aliye has contributed significantly to strategy and product development, including building IBM's eDiscovery business unit. She holds Bachelor's and Master's degrees in Computer Science and an MBA in Marketing and Entrepreneurship from the Australian Institute of Business (AIB).

Arthur Sitaramayya

Senior Business & Delivery Leader – Information Technology

Arthur Sitaramayya, a seasoned Senior Business & Delivery Leader in Information Technology, brings a wealth of experience in business and technical leadership across multiple industries globally. He has successfully transformed and delivered services internationally, demonstrating strong client engagement skills. Arthur specialises in establishing, managing and growing service delivery teams of various sizes in centre-based and client-facing roles. He is dedicated to aligning IT value with business outcomes, emphasising strategic management and people leadership. Recently, he enhanced his expertise by earning an MBA from the Australian Business Institute in December 2022, underscoring his commitment to continuous knowledge growth.

Cite this article:

Charitsis, V, Jeffrey, S, Ozcan, A, Sitaramayya, A 2023, 'Generative Artificial Intelligence Reshaping Business: Adapting Cybersecurity Strategies for the New Era', *AIB Review*, Issue 11.

Explore more articles from AIB Review