


Data Breaches: FIGHT AI WITH AI

Mohammad Rajib Uddin¹, Shahriar Akter¹ ,
Wai Jin (Thomas) Lee¹, and Shlomo Y. Tarba²

California Management Review
2025, Vol. 68(1) 160–173
© The Regents of the
University of California 2025
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/00081256251377346
journals.sagepub.com/home/cm



SUMMARY

AI-driven data breaches are escalating as personalized phishing, deepfakes, and disinformation proliferate. While research has focused on post-breach responses, the defensive capabilities firms need remain unclear. This study examines how companies can build AI-powered dynamic capabilities to anticipate, withstand, and counter emerging, unpredictable AI-generated threats.

KEYWORDS: data management, decision making, digital technology, organizational culture, technological change, artificial intelligence

KEY RECOMMENDATIONS

- **Build an AI-centered security culture:** Make AI literacy and security awareness part of every employee’s daily practice.
- **Lead ambidextrously, balancing today’s defenses with tomorrow’s innovations:** Invest simultaneously in robust basics and forward-looking AI defenses.
- **Treat training as a permanent campaign, not a project:** Run continuous, evolving security drills and awareness programs for everyone, including leadership.
- **Turn governance into a competitive advantage:** Treat encryption, access control, and selective data sharing practices as proactive value drivers.

The rise of Generative Artificial Intelligence (Gen AI) has introduced extraordinary capabilities for businesses and has been the spotlight of the current AI revolution. As different Gen AI models continuously foster new capabilities, the cyber risk associated with them cannot be ignored.¹ “In the past few years,

¹University of Wollongong, NSW, Australia

²University of Birmingham, Birmingham, UK

cybercriminals have been using AI to disrupt businesses, and now the introduction of generative AI is bringing new challenges for businesses.² Cyber attackers can utilize such models to breach businesses through sophisticated attacks, rendering traditional defense methods obsolete. Businesses must, therefore, foster better people and adapt to new technologies.³

Cybercriminals use sophisticated attacks daily, and the introduction of Gen AI adds a massive firepower boost to their arsenal.⁴ Using Gen AI, criminals can impersonate individuals through email and telephone calls, thereby compromising sensitive information. For example, perpetrators can use Gen AI tools to create convincing social engineering attacks, such as phishing or an attack payload. It is essential to recognize that Gen AI's ethical policies prohibit users from misusing the technology. However, there are ways to bypass these policies through jailbreaking and reverse psychology techniques. Furthermore, malicious actors can use AI models to automate hacking procedures or to find vulnerabilities in a system for exploitation.⁵ For example, over 2,322 unauthorized money transfers in Japan occurred via the Internet in 2023, where perpetrators used state-of-the-art AI technologies, highlighting the growing tension of AI-driven cybercrimes.⁶ Indeed, AI-based data breaches are often more severe than traditional data breaches due to the sophistication of technology (e.g., deep learning model-driven deep fake content, automated phishing emails, hyper personalized and optimized threats, automated reconnaissance, model poisoning, prompt injection, or tailored social engineering attacks). Therefore, this new and disruptive threat requires more investigation and research. Table 1 provides a snapshot of AI-related data breach incidents in recent times.

Data breaches resulting from cyberattacks can cause severe reputational and financial damage to a business. A data breach can occur when sensitive information is intentionally or unintentionally compromised. In Australia, data breaches and cybercrimes have recently gained massive momentum. Criminals are breaching big brands and stealing millions of customers' personal information, such as contact information and financial and medical information. Australian consumers now prioritize protecting their information when choosing a product or service. According to the ASD 2023 report, stolen customer data from an entity in Australia can be used for various malicious purposes, including identity theft, blackmail, or extortion.⁷ While governments and businesses are taking initiatives in Australia to protect their consumers' information, data breaches and cybercrimes are still rising. With the evolution of technologies, data breaches are becoming increasingly dynamic. To mitigate this issue, businesses must establish dynamic capabilities for timely sensing and responding to unexpected changes in the business environment.⁸ Indeed, Goel et al. argue that the proper use of advanced technologies and proper action by individuals is significant when responding to and recovering from information security-related issues; thus, firms can benefit from achieving dynamic capabilities.⁹

While dynamic capabilities provide the ability to create, modify, and transform a business's internal and external resources in a rapidly changing

TABLE I. GenAI-Related Data Breach Incidents.

Incident Types	Organizational Impacts
Deep fakes voice	A <i>Forbes</i> article depicts that a chief executive officer's voice was mimicked by Deepfake using artificial intelligence to heist \$243,000. This incident shocked tech experts as it was the first time a convincing Deepfake voice was used to scam. ^a
Deep fake videos	According to Hong Kong police, a financial firm paid \$25 million to fraudsters after an employee was scammed using deep fake video and voice. The worker attended an online meeting where he could recognize all his colleagues in the video conference; however, everyone was fake in the video conference. ^b
Disinformation	According to <i>MIT Technology Review</i> , around the world, politicians and governments are using Gen AI text images and videos to manipulate public opinion. The government is censoring critical information using Gen AI and only providing information that favors them. ^c
Phishing Emails	Attackers are now using Gen AI to create more convincing emails, which is causing havoc among businesses and their stakeholders, such as suppliers or third-party vendors. With Gen AI, perpetrators can now use phrases and information that mimic an actual employee, convincing the victim to gain access to sensitive information or fund transfers. ^d

^a"Analyzing the rise of deepfake voice technology," *Forbes*, May 10, 2021, <https://www.forbes.com/sites/forbestechcouncil/2021/05/10/analyzing-the-rise-of-deepfake-voice-technology/?sh=20f80a486915>.

^b"Finance worker pays out \$25 million after video call with deepfake 'chief financial officer.'" CNN, February 4, 2021, <https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>.

^c"How generative AI is boosting the spread of disinformation and propaganda," *MIT Technology Review*, October 4, 2024, <https://www.technologyreview.com/2023/10/04/1080801/generative-ai-boosting-disinformation-and-propaganda-freedom-house/>.

^d"AI linked to new crop of business email scams," *CybersecurityDive*, June 29, 2023, <https://www.cybersecuritydive.com/news/ai-business-email-scams/654092/>.

environment,¹⁰ a microfoundation, on the contrary, is responsible for developing dynamic capability through individual and/or organizational processes and collective actions.¹¹ Given the uncertain nature of data breaches, our goal is to explore the microfoundations that are needed for firms and individuals to be dynamic in response to data breach threats. Therefore, our work revolves around the following question: What are the microfoundations of data breach protection capabilities in the Gen AI environment?

Methodology

In Phase 1, we reviewed over 100 data breach cases across Australia and worldwide. Analyzing the case studies helped us understand Australia's data breach environment in comparison to the rest of the world. In Phase 2, we conducted a qualitative study using in-depth interviews with 26 experts specializing in cybersecurity, data management, and AI. The interviews were with various organizations from different industries, including Fortune 500 companies. While most of our participants were from Australia, we also had the opportunity to interview experts from the United States. Each interview lasted 40 to 60

minutes, providing valuable insights into the current challenges of data breaches and what needs to be done to achieve ultimate protection. Finally, we designed and distributed a survey for 300 industry experts. The survey helped us confirm the findings of our qualitative explorations. Our results indicate that businesses must adopt AI-powered dynamic capabilities, utilizing organizational, talent, and technological resources, to thrive in a dynamic threat environment. The study identifies eight microfoundations across organizational, talent, and technological capabilities, which are discussed in the following sections.

Organizational Capabilities

Our findings underscore the significance of AI-powered security culture, the adoption of benchmarking practices, and the vital role of ambidextrous leadership as foundational elements in developing organizational capabilities to address the threats posed by data breaches.

AI-Centered Security Culture

AI-centered security culture identifies AI as a core component in strategies, processes, and mindsets to prevent, detect, and respond to data breaches. It prepares everyone, from leaders to individual employees, to understand, leverage, and responsibly manage AI in the context of threats (e.g., automated responses, predictive capabilities, proactive threat detection, and continuous learning). Establishing such a culture of security is one of the most critical steps for an AI-driven business. For meaningful change, simply telling employees what to do rather than what not to do will not be enough; understanding what people do when no one is looking is also very important. Yahoo takes several small steps daily to enhance employee security behavior, such as offering short courses, addressing specific behavioral goals, and continually working to develop employees' security behavior.

Our participants heavily emphasized the importance of an AI-ready culture and thoughtful change management to establish security implications. A company's culture can predict a particular data breach, so a firm must promote a learning culture where employees are encouraged to learn new things. Culture is the most critical aspect because it is where the problem begins, and where the issue of data breaches often arises. Hence, firms must strive to change their culture slowly. They should not change culture rapidly, as this can demotivate people and cause trouble in daily operations. We must remind ourselves that good things take time.

Benchmarking, Audits, and Best Practices

In an AI-driven threat landscape, benchmarking must evolve beyond traditional models to account for AI's dynamic capabilities—both as a defense and a threat. For example, it is crucial to benchmark response time, detection rate, and employee susceptibility to threats against industry peers, such as AI-generated phishing, deepfake impersonations, and synthetic data leaks. For example, Taylor Fry, a leading analytics and actuarial consulting firm, relies heavily on benchmarking to improve its cybersecurity performance. Firms should benchmark

everything from technology to policies and audit their security measures every three months. Benchmarking can help a business better understand its own position and that of the vendor in terms of security.

To adopt best practices, businesses must emphasize the importance of comprehensive security across all aspects. Each department should be responsible for its safety and work together. Employees should be encouraged to use stronger passwords, avoid leaving their workstations unattended without proper security measures, and exercise caution when working with third parties.

Ambidextrous Leadership

Ambidextrous leadership in the AI landscape refers to the ability to balance exploration (innovation) and exploitation (operational efficiency) to defend current threats as well as to prepare for the unknown, evolving ones. To be resilient today and adaptive tomorrow, an ambidextrous leader should encourage proactive investment in AI security tools (e.g., deep fake detection) as well as ensure robust foundational practices (e.g., encryption) and response procedures (e.g., autonomous response systems). The more leaders understand about information threats, the better they can comprehend their impact on the organization's strategy and risks.¹² The head of information security at HS Prevent, an anti-fraud solution company in Brazil, states that in a world where change is the only constant, leaders must gain the ability to explore new technologies, remain vigilant to changes in the threat landscape and find ways to innovate without compromising existing operation, this is what a trait of an ambidextrous leader should be in a changing threat environment.¹³

Leaders need to encourage managers to become proactive and stay current. Leaders should not have a profit-only mindset; instead, they must adopt a mindset that emphasizes enhancing employees' competencies in understanding security and staying current on security-related issues. Many upper-level managers continue to view data breach-related problems as primarily a technological issue. However, it is essential to understand that a data breach is a business risk that requires strategic investment; without it, a company might be investing in the wrong security area. This is what a few companies have done wrong; they lacked strategic investment. All the technology in the world will not save a business from a breach. For example, the NSA (National Security Agency) spends billions on technology, yet it still gets breached. All it takes is for someone to click on a nasty email or answer a phone call and become a victim of social engineering. An establishment can only change if its leaders first take the initiative to change themselves and assume more responsibilities.

Talent Capabilities

Our findings reveal the critical role of talent in enhancing organizational security. Talent capability refers to an individual's ability to help a business secure itself from disruptive threats caused by any AI element. Our findings identify the critical roles of training and awareness, competence, and teamwork as micro-foundations in developing talent capabilities.

Training and Awareness

Regular training is vital to enhance awareness. The firm must find new and innovative ways to change everyone's behavior to establish more effective data breach defense practices. Regular security training is critical for employees at all levels. The goal is to ensure the staff are empowered and understand the threats better, which can eventually improve the company's security posture.

We must understand that training and awareness programs cannot be a project. They must run regularly and be innovative, as people tend to avoid training at work because it adds another task to their daily list. The programs should be updated periodically as new patterns of threats are emerging. A data security expert from our interview suggests that firms should conduct drills for data breaches, like fire safety drills. Everyone, from the CEO to the janitor, should participate in training and awareness programs, as even janitors are responsible for handling the company's assets. As people are our first line of defense and targets, an ongoing awareness campaign should be implemented. This campaign can raise awareness regarding the understanding of AI-generated phishing emails and encourage employees to take care of their equipment, such as laptops. It is essential to understand that technology alone cannot defend a business; hence, user awareness and training are top priorities.

Competence

Along with sophisticated automated technologies, human presence and talent are needed to monitor threats. As we all know, hackers are not automated; therefore, businesses must have talented personnel in place. Automated technologies, such as Gen AI, will not help, as hackers also possess similar technologies. People need to be more dynamic because hackers are dynamic. Hence, we need specialists to constantly monitor activities and understand the patterns of emerging threats.

A cybersecurity expert at a Fortune 500 company states that they ensure human presence 24/7 and advise against over-reliance on advanced technology, such as AI and Gen AI, after learning a valuable lesson from a previous breach. He further points out that there is a talent gap in the market as threats are evolving faster than we can improve talent; hence, continuous learning is necessary. However, even if an employee possesses the right talent for securing business information, businesses might still not be secure if the individual lacks the motivation to protect the company's information and assets. Hence, employers must determine if an individual is aware of the risk.

Teamwork

A data breach is a crisis, and teamwork during a crisis is essential not only to mitigate the risk, but also to contain it. Specifically, in an AI environment, threats are multifaceted as they involve technology, human behavior, compliance, and ethics. Thus, a collaborative, cross-functional team is essential across cybersecurity, IT, legal, HR, data science, and communications teams. Within an entity, people must strive to be better team players and support one another.

Better teamwork and communication should be established between every team and department. For example, the collaboration between IT and security teams should be extended to the rest of the organization. The rest of the organization often neglects the IT and security teams as they tend to disrupt operational activities, which can irritate staff members; however, this mindset must change, and security experts must improve how they communicate with other teams, as IT professionals often tend to have weak communication skills with the rest of the organization. The contribution and importance of the security team needs to be highlighted and emphasized, now more than ever.

Technological Capabilities

Technological capability is the critical infrastructure of an organization to address data breach threats, which is essentially based on two microfoundations: data governance and technological sophistication.

Data Governance

Ensuring proper data governance has become vital as companies shift toward using more AI-related products. It is the company's responsibility to ensure data safety, and that proper data care comes from reliable platforms and technologies. Regarding proper data management, experts suggest that we must have security methods in place across all stages of data collection, storage, handling, and archiving in the Gen AI environment. Unnecessary data should be deleted, data should be stored in various locations, and sensitive data should be separated from other data. When working with data, departments should only use data that is necessary and central to their operations. For example, marketers use data to identify segmentation and targeting; however, this data can become vulnerable, as it is also transmitted to a third party for analysis. Hence, marketing must be extra cautious. Marketers need to delete the data after the work is done. Caution should be exercised when sharing data with third-party vendors; it is also advisable to investigate the security practices of these vendors.

Data encryption and proper access control are among the most critical security factors in data governance. Encrypt your data; it must be encrypted if your company deals with the public's data. Sometimes, breaches happen through unintentional actions. For example, you send data to a third party without proper encryption.

Technological Sophistication

Firms must appreciate the importance of investing in technology, including acquiring specific software applications, making the necessary upgrades, and assessing their potential vulnerabilities against current threats. For example, to counter threats generated by Gen AI, firms must deploy Gen AI capabilities in conjunction with human input and involvement. Owing to the unique and volatile nature of cybersecurity threats, a one-size-fits-all approach may not be appropriate, and firms must remain vigilant by testing innovative technologies against potential vulnerabilities.

AI and machine learning capabilities can immensely boost security platforms. They can help detect and respond to threats more quickly and accurately, making the responsibilities of cybersecurity professionals easier. Companies like PayPal, Visa, and MasterCard utilize machine learning capabilities to enhance their data security.

A senior technical manager at a leading AI-based cybersecurity company asserts that, given the rapid evolution of AI, companies must stay ahead of the curve. Otherwise, they will fall behind and lose everything. Firms must have robust technology to address Gen AI-centered security concerns; they must identify the right person and possess the necessary instruments and strategies.

Experts suggest that to implement AI capabilities successfully, entities must deploy machine learning and deep learning capabilities to analyze data and identify abnormalities within the dataset. For automation, deep learning can be used to identify trends and predict potential threats. Natural language processing can help security managers perform their tasks more efficiently and make them more proactive.

Pathways to the Future

Drawing on our research findings and suggested policy recommendations, we have assessed the data breach environment in the Australian banking, retail, telecommunication, and healthcare industries. Our assessment and overall findings identify two types of companies: *adopters* and *non-adopters* of data breach protection capabilities in the AI threat environment.

Table 2 exhibits *adopters* who stay ahead of the curve by effectively developing their organizational, talent, and technological capabilities. The findings showcase the AI-powered data breach protection environment of one of the top four banks, a major retailer and a global financial service provider in Australia. The security practices of these firms have embraced our holistic guidelines and developed dynamic capabilities through the operationalization of various micro-foundations (e.g., ambidextrous leadership, competence, and technological sophistication).

Table 3 presents *non-adopters* who have failed to protect against data breaches due to the non-adoption of holistic security guidelines, as suggested in our findings. These firms were unable to adapt to the changing environment, and their leaders also failed to recognize the critical nature and impact of data breaches in the era of AI. Our findings reveal that a major telecommunications company suffered unauthorized access to approximately 9.8 million customer records. Similarly, a prominent health insurance provider experienced a data breach, compromising the personal information of 9.7 million patients. In addition, a leading prescription service provider lost the medical data of 12.3 million customers due to advanced ransomware attacks that leveraged AI. Thus, we reiterate the critical role of AI in augmenting traditional defense methods and rule-based training in developing robust capabilities across the organization, talent, and technology.

TABLE 2. Adopters of AI-Powered Data Breach Protection Capabilities.

Organization	Adoption of Recommended Capabilities	Benefits
<p>One of the top 4 banks in Australia</p>	<p>1. Organizational Capabilities <i>Ambidextrous Leadership:</i> The bank ensures that the leaders and managers are well-educated in data privacy and security. They are trained to detect employee behavior, and they ensure their team plays a critical role in data management and abides by safety protocols. They ensure that data is only accessible to authorized team members.</p> <p><i>Best Practices/Training and Awareness:</i> The bank has moved beyond its traditional compliance training program and is now taking more creative initiatives for its diverse employees. Engaging learning programs are used to develop employee knowledge of security and change their digital habits.</p> <p>2. Talent Capabilities <i>Competence:</i> The firm ensures that the employees are able to protect information. During the selection process, employees in all departments are screened to identify those with a better understanding of protecting organizations and their customers' information.</p> <p>To enhance their security teams, the top four banks not only recruit top security engineers, but also have most of their senior cyber managers from diverse backgrounds, including business administration and economics. Over 90% of attacks involve multiple departments, and they continue to evolve on a daily basis. The diverse cyber team helps customers stay safe and continues to defend the bank.</p> <p>3. Technological Capabilities: Employees are only allowed to use networks and technologies provided by the bank and are discouraged from working from home due to security concerns. The bank has implemented AI for enhanced threat detection and is aware of the ongoing advancements in AI technologies. They also ensure that security specialists are available 24/7.</p>	<ul style="list-style-type: none"> • Enhanced customer trust through better data protection • Fostered a better security environment through establishing a culture of learning • Improved relationships with all stakeholders, demonstrating stronger cyber resilience
<p>A major retailer in Australia</p>	<p>4. Organizational Capabilities: <i>Culture/Benchmark:</i> The retail giant has assigned a security expert to every team, ensuring that the expert can raise awareness among all its members and provide a benchmark for everyone to follow. This has ensured the development of a proper security culture. The firm took years to develop a sense of security for protecting stakeholders' information.</p> <p>5. Talent Capabilities <i>Training and Awareness:</i> Employees are encouraged to participate in interactive simulations. These simulations not only foster their knowledge regarding cyber threats but also develop a healthy team. The simulations are like games that every team must finish every week. While gamification, such as hackathons, has become a part of Australian retail giants, firms must be careful not to use actual customers' information, as accidents can happen.</p> <p>6. Technological Capabilities <i>Technological Sophistication:</i> The firm ensures not only that its technology is up to date but also that the security systems of its third-party vendors meet its standards. The security team continuously monitors the entire system with the help of their advanced AI system. All platforms are monitored from the cloud to the point of sale.</p> <p>Australian retail companies are increasingly becoming tech companies, as the number of customers using their digital platforms is growing rapidly. Retailers are now utilizing Gen AI to help customers make informed purchasing decisions and receive personalized recommendations and customer service.</p>	<ul style="list-style-type: none"> • Boosted teamwork through training activities • Increased productivity through better interaction • Provided better protection and greater service through an online platform, resulting in greater customer acquisition • Enhanced trusting relationships with vendors and suppliers lead to long-term good relationships, benefiting both parties

(continued)

TABLE 2. (continued)

Organization	Adoption of Recommended Capabilities	Benefits
<p>A global financial services company</p>	<p>1. Organizational Capability <i>Best Practice:</i> Continuously monitor the cyber threat landscape to gain knowledge of potential threats and implement effective strategies for managing them. The firm uses its operational risk management framework, which is kept updated. <i>Culture:</i> The firm boasts a highly performing culture and a diverse and inclusive team. People in the organization are nurtured in a way that enables them to adapt quickly, think critically, and learn effectively while ensuring that employees are valued.</p> <p>2. Talent Capability: <i>Training and Awareness:</i> A dedicated, specialized team is kept in-house to oversee the threat landscape and train all staff. The dedicated team ensures the software is updated, researches current risk issues, and manages and destroys data. <i>Teamwork:</i> The group has a risk operational manager for every team, who ensures safe operational activities daily and helps the team work efficiently.</p> <p>3. Technological Capability: <i>Technological Sophistication:</i> The financial service invested heavily in staying updated with leading technologies to address the growing data breach landscape. In terms of data privacy, the firm does its best to protect customer data throughout its life cycle, ensuring security for customers' data from collection to destruction. The firm does not use too many tools for securing its cyberspace. They use limited and efficient tools, such as an extended detection and response platform. The banking and financial services holding of the group runs 96% of its applications on the public cloud, which also includes its core banking platforms. This enables the firm to offer better customer service and security on its digital platform.</p>	<ul style="list-style-type: none"> • Enhanced customer privacy and security by leveraging advanced cybersecurity and technologies • Ensured better harmony and agility among team members • Nurtured employees to be more dynamic. Facilitating faster decision-making in daily operations and in cyber warfare

TABLE 3. Non-Adopters of AI-Powered Data Breach Protection Capabilities.

Organization	Incident	Result	Cause	Recommendation
Top telecommunication firm in Australia	Unauthorized access due to unsecured application	Over 9.8 million customer records were accessed, which included personal information such as driver's licenses.	Experts believe that the firm did not sufficiently prioritize the customer's data. This can happen due to management negligence. An unsecured application means that the IT team was not aware of the present landscape of data breaches.	<ul style="list-style-type: none"> The firm needs a security mindset that extends from the top to the bottom of the organization. They need to keep their technological capabilities up to date. Top management must understand the value of customer data and the importance of protecting it. The firm needs to establish a more robust cybersecurity team that will oversee the threat landscape and provide hands-on training to every team.
Top health insurance firm in Australia	Unauthorized access through theft of credentials	<p>Hackers could access the firm's platform by stealing the credentials of a third party.</p> <p>Hackers accessed over 9.7 million customer's sensitive information, including health-related information.</p>	<p>Multifactor authentication was not in place, so hackers used malware to obtain credentials from a person with privileged access.</p>	<ul style="list-style-type: none"> The firm can learn about proper access control from the top 4 banks in Australia. The firm can implement strict access control within its platform and ensure that even individuals with privileged access must undergo a rigorous security system. The firm needs to stay ahead of hackers in this dynamic threat environment, where hackers are constantly up to date with new technologies.

(continued)

TABLE 3. (continued)

Organization	Incident	Result	Cause	Recommendation
A prescription delivery service in Australia	Unauthorized access to a server using ransomware	Hackers used ransomware attacks and stole over 12.3 million customer's sensitive information, including medical data. Its breach was the largest to date in Australia.	Ransomware attack	<ul style="list-style-type: none"> • It needs to keep its system updated. • Heavy investments are needed to secure their platform. • Training and awareness should be the top priority among the employees. • The board must prioritize information security because change can only occur if the board changes its view.

Conclusion

Firms worldwide need to fully understand both the threats that AI poses and the possibilities it offers. To address the persistent threats of data breaches in the era of AI, firms must adopt an AI-powered security culture, benchmark their technological protocols, cultivate a learning and growth mindset, and prioritize the competence of their talent. AI has the potential to create a world of deception, and data breaches could become more frequent and dangerous. A holistic focus on organizational, talent, and technological capabilities can empower firms to thrive in a rapidly changing landscape.

Author Biographies

Mohammad Rajib Uddin is a Doctoral Candidate in the data breach research cluster at UOW, Australia. He has extensive consultancy experience in cybersecurity, having served in various roles as a team coordinator and senior executive (email: muddin@uow.edu.au).

Shahriar Akter is a Professor of Marketing Analytics at UOW, Australia. He earned his PhD from UNSW Business School, Australia, with a fellowship from the University of Oxford. He has published in leading business journals, including *CMR Insights* (email: sakter@uow.edu.au).

Wai Jin (Thomas) Lee is a Senior Lecturer in Marketing at the School of Business, Faculty of Business and Law, University of Wollongong. He earned his PhD from the University of Tasmania, Australia (email: thlee@uow.edu.au).

Shlomo Y. Tarba is a Chair in Strategy and International Business at the University of Birmingham. He is an internationally recognized scholar in the field of corporate strategy. He serves as an Associate Editor of the *Journal of Product Innovation Management* and is a member of the international review board of *CMR* (email: s.tarba@bham.ac.uk).

Notes

1. M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," *IEEE Access*, 11 (2023): 80218-80245, <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10198233>.
2. K. Renaud, M. Warkentin, and G. Westerman, "From ChatGPT to HackGPT: Meeting the Cybersecurity Threat of Generative AI," *MIT Sloan Management Review*, April 8, 2023, <https://sloanreview.mit.edu/article/from-chatgpt-to-hackgpt-meeting-the-cybersecurity-threat-of-generative-ai/>.
3. Renaud, Warkentin, and Westerman (2023), op. cit.
4. "How Cybercriminals Are Using Gen AI to Scale Their Scams," *Okta*, January 4, 2024, <https://www.okta.com/blog/2024/01/how-cybercriminals-are-using-gen-ai-to-scale-their-scams/>.
5. Gupta et al. (2023), op. cit.
6. "Generative AI Contributes to Increase in Cybercrimes," *Nikkei Asia*, January 7, 2024, <https://asia.nikkei.com/Spotlight/Datawatch/Generative-AI-contributes-to-increase-in-cybercrimes>.
7. "ASD Cyber Threat Report 2022-2023," *Australian Government/Australian Signal Directorate*, November 14, 2023, <https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023>.
8. F. Khan, J. H. Kim, L. Mathiassen, and R. Moore, "Data Breach Management: An Integrated Risk Model," *Information & Management*, 58/1 (January 2021): 103392.

9. L. Goel, D. Russell, S. Williamson, and J. Z. Zhang, "Information Systems Security Resilience as a Dynamic Capability," *Journal of Enterprise Information Management*, 36/4 (February 2023): 906-924.
10. D. Teece, M. Peteraf, and S. Leih, "Dynamic Capabilities and Organizational Agility: Risk, Uncertainty, and Strategy in the Innovation Economy," *California Management Review*, 58/4 (Summer 2016): 13-35.
11. D. Bendig, S. Strese, T. C. Flatten, M. E. S. D. Costa, and M. Brettel. "On Micro-Foundations of Dynamic Capabilities: A Multi-Level Perspective Based on CEO Personality and Knowledge-Based Capital," *Long Range Planning*, 51/6 (December 2018): 797-814.
12. M. Parent and B. H. Reich, "Governing Information Technology Risk," *California Management Review*, 51/3 (Spring 2009): 134-152.
13. A. V. de Oliveira, "Ambidextrous Leadership in IT and Cybersecurity: Balancing Innovation and Stability," *CIO Applications*, 2024, <https://www.cioapplications.com/cxoinsights/ambidextrous-leadership-in-it-and-cybersecurity-balancing-innovation-and-stability-nid-10973.html>.

ORCID iD

Shahriar Akter  <https://orcid.org/0000-0002-2050-9985>