









Inside the Threat Matrix: Using Hybrid Computer Simulations to Educate Adults on Malicious Insider Threat and Technology Misuse

Monica T. Whitty^(✉) , Dinislam Abdulgalimov , Patrick Oliver ,
Christopher Ruddy , Joshua Seguin , and Garry Young 

Faculty of IT, Monash University, Melbourne, VIC 3800, Australia
monica.whitty@monash.edu

Abstract. With the ever-evolving Internet and the use of digital technologies in work and play, there is a critical need for adults to understand its usage and, with respect to cyber security, how others might exploit technology. In this study, we created a malicious insider training and education hybrid computer scenario which organisations could use to train employees. This paper considers how these simulations might be employed to train and educate adults about the misuse of technologies through the example of a malicious insider threat hybrid computer simulation study designed to educate employees and policymakers. It also considers the ethics of employing hybrid computer simulation methods to educate adults about these behaviours. Drawing from Mezirow’s ‘Transformative Learning Theory’, the paper demonstrates the utility of this method, drawing from his principles of disorienting dilemmas, critical reflection and action. It also elucidates that some learners are more likely to engage in self-reflection, whilst others are more likely to consider the ‘other’ and how this perspective must be considered in the learning process. It is concluded that hybrid computer simulations are a highly effective way to teach and train employees about criminal and problematic misuse of technology.

Keywords: Malicious insider threat · Hybrid computer simulations · Education and training · Technology misuse · Cyber security

1 Introduction

Insider threats pose a significant threat to businesses (Whitty 2021). Educating and training employees about accidental insider threats are not uncommon – although much research is still needed to improve these methods’ effectiveness (Khando et al. 2021; Whitty et al. 2024a, 2024b). Research on effectively educating and training employees about malicious insider threats is even rarer. Most of the work in this area involves raising awareness of malicious attacks and improving security policies to reduce the risk of these attacks (Greitzer et al. 2008). This paper offers a novel approach to training employees

and policymakers on insider threats using a hybrid computer simulation method. In particular, the paper reports on an innovative method we developed to train people on IP theft. We draw upon Mezirow's 'Transformative Learning Theory' to explain why this method has much potential for training adults and how this might be extended to other types of technology misuse, such as scams, trolling, bullying and sabotage.

1.1 Background

A malicious insider attack is a security breach perpetrated by individuals within an organisation who misuse their authorised access for harmful purposes (Cappelli et al. 2012; Whitty, 2021). These individuals exploit their trusted position to engage in activities such as data theft, espionage, sabotage and fraud. Unlike external attackers, insiders inherently hold a position of trust and familiarity with internal systems, making their actions particularly difficult to detect and mitigate. Notably, their actions are more commonly detected externally (e.g., reports to the organisation) than internally (Whitty 2021).

The study of malicious insider threats examines how to detect, prevent, and disrupt these attacks within organisations. Models have been developed to analyse patterns (technical and human) to identify potential indicators of insider threats (e.g., Nurse et al. 2014; Liu et al. 2018; Whitty 2021; Whitty et al. 2023, 2024a, 2024b). Whitty et al. (2023, 2024a, 2024b) have identified distinct socio-technical events in different insider attacks. Research has also identified the role of organisational culture in either mitigating or exacerbating these threats (Sarkar 2010).

Some organisations, such as defence and critical infrastructure organisations, train managers to recognise the signs of potential malicious insiders (Nelson et al. 2019). Ironically, insiders' peers more than managers recognise malicious workplace behaviour (Whitty 2021). What often prevents reporting, however, is a lack of confidence in employees' observations and fears around confidentiality in the reporting process (Bell et al. 2019). Researchers have concluded that organisations must provide effective training regarding behavioural indicators of insider threats (Bell et al. 2019; Nurse et al. 2014; Whitty 2021).

Objectives. The main objective of this research is to examine the utility of a hybrid computer simulation method for educating and training employees about malicious IP theft. A secondary aim is to draw from these findings to suggest how these methods might be employed to educate and train adults about other types of technology misuse (e.g., scams, trolling, bullying, and sabotage).

1.2 Theoretical Framework

Until the 1970s, adult learning was considered the same as educating children. Knowles' (1978) work on 'andragogy' shifted scholarly thinking around adult learning compared to child-focused education. Andragogy has six assumptions: (a) self-directedness, (b) need to know, (c) use of experience in learning, (d) readiness to learn, (e) orientation to learning, and (f) internal motivation (Knowles 1978; Sang 2010). According to Knowles, adults are self-directed learners who bring a wealth of life experiences to the learning process, which serves as a valuable resource for building new knowledge. Knowles

defined the art and science of adult learning, emphasising the importance of autonomy, practical application, and experiential learning (Knowles 1978; Clair 2024). The theory has been widely adopted in digital and professional education (Greene and Larsen 2018).

Despite its utility, andragogy has its critiques. Some argue that it oversimplifies the diversity of adult learners (Stancil 2025). Knowles' work has also been criticised for neglecting to include empirical evidence and failing to account for cultural, content, and individual differences (McGrath 2009). Clair (2024) argues that andragogy does not fully address the needs of learners from diverse cultural or socioeconomic backgrounds.

Since Knowles' time, scholars have reworked his principles to develop the 'Transformative Learning Theory' (Mezirow 2018). This theory posits that adults learn by critically reflecting on their experiences, challenging their assumptions, and ultimately transforming their perspectives and understanding of the world. This process, often sparked by a disorienting dilemma, involves self-reflection, dialogue with others, and the integration of new beliefs that lead to meaningful personal growth and behavioural change. Therefore, Mezirow's (2018) Transformative Learning Theory is ideal for informing educational practices around learning about cyber security concerns around technology misuse. Based on these principles, this theory suggests that computer simulation studies are favourable for adult learning (Clapper 2010).

Mezirow's theory has been mainly applied in healthcare education, where computer simulations have been developed to simulate complex patient scenarios. According to the theory, reflective debriefing sessions integrated into these simulations are essential for fostering perspective transformation among participants. For instance, Almomani et al. (2023) demonstrated how reflective learning conversations in healthcare simulations enhanced clinical reasoning and empathy among participants. Similarly, Gum et al. (2010) found these training techniques helpful for the midwives, doctors and nurses who participated in their study. They claimed that in addition to learning new content, participants learned how to collaborate, team build, and ultimately become more focused on clinical practice outcomes. Perhaps not surprisingly, McCaughey and Traynor (2010) highlight that these mock clinical simulations are ethical, given that they can minimise patient harm.

1.3 Computer Simulations

Computer simulation studies and methods to train people are not common in cyber security. However, more recently, they have been suggested as a way forward in training employees (Dunphy et al. 2014; Kavak et al. 2021). Studies have been designed to examine how human defenders learn to counter simulated adversaries in interactive cyber-defence games (Prebot et al. 2023). Computer simulation training has been developed to improve phishing susceptibility (Shin et al. 2023). To our knowledge, no studies have developed computer simulations for participants to *educate* adults about malicious insider attacks.

Computer simulations are more commonly designed to teach practical skills in safe environments, such as pilot (Hight et al. 2022), teaching (Kelleci et al. 2020) and medical training (Basyuk et al. 2024). These studies, however, teach skills rather than require participants to engage in critical reflection. More recently, computer simulations have

been proposed as a method for transformative learning, for example, seeing the world through the eyes of diverse populations (Soilis et al. 2024).

Hybrid computer simulations have also gained prominence as innovative tools for adult education and training. By integrating virtual environments with human-mediated communication, these simulations allow learners to engage in collaborative, realistic, and immersive learning experiences (Gudoniene et al. 2025). Arguably, the inclusion of human communication enhances the realism and social aspects of the learning experience, which are critical for learning (Bell and Kozłowski 2008). This current study developed a *hybrid computer simulation*, giving us control of the scenario and allowing for a more authentic and immersive learning experience.

1.4 Summary

Our paper, therefore, offers a novel approach to training employees to understand insider threats and more effectively detect malicious insider threats within their organisations. The work we present developed a hybrid computer simulation study where participants could choose to play out an insider or resist external attempts to recruit them as malicious actors in a fictitious scenario. A realistic scenario was developed to provide participants with an immersive and potentially reflective experience in a safe environment over 3 phases. It drew from insider threat research designed to detect deception language in a face-to-face scenario (Taylor et al. 2013).

In accordance with Mezirow's Transformative Learning Theory, we developed hybrid computer simulations that promote transformative learning. At its core, transformative learning involves a process of reflection and re-evaluation, enabling individuals to shift their worldviews in meaningful ways. Computer simulations designed with this theory can create immersive, dynamic environments where learners are prompted to confront their preconceptions. This can potentially help with complex scenarios, such as malicious insider threats, and expose users to alternative perspectives and unanticipated outcomes, fostering a deeper understanding.

2 Methods

2.1 Participants

A total of 15 university students aged 21–33 years, with a Mean age of 25 years ($SD = 3.29$), participated in the study. Six participants chose to play the role of an insider, and nine decided not to play an insider. We recruited students who would be more likely to be interested in the scenario by inviting those with an interest or background in communications (digital/media), marketing, or cyber security.

2.2 Procedure

For this study, we designed a hybrid computer simulation that attempted to mimic a real-life work situation with known steps that can occur leading up to an IP theft attack (Whitty et al. 2023, 2024a, 2024b). The simulation was designed based on the principles

of Transformative Learning Theory (Mezirow 2018). Akin to other computer simulations that draw from this theory, reflective debriefing sessions were integrated into these simulations. This paper examined these reflections to elucidate what type of learning (if any) occurred.

We created three rounds in the scenario, each lasting approximately 100 min, to provide participants sufficient time to perform work and insider tasks while limiting the risk of participant fatigue. During the initial briefing, the participant was asked not to engage in any personal activities during the simulation and encouraged to regularly check the inbox of the email account assigned to them. The participant was directed to the organisation tab on Microsoft Teams, where each coworker's details could be viewed. An organisational chart was provided.

Prospective participants were recruited via advertisements. They were offered a voucher valued at \$210 as compensation for their time and were advised that additional financial incentives may also be presented during the simulation. The first round was designed to establish a behavioural baseline. In rounds 2 and 3, the participant could opt to be an insider and was paid \$50 if they engaged in IP theft in round 2 and an additional \$50 if they were successful in round 3. If participants opted not to be insiders in round 2, they were offered double the amount (\$100) in round 3 if they decided to engage in an attack. Furthermore, all participants were paid \$50 for engaging in the study.

The study was designed according to ethical guidelines, ensuring confidentiality and anonymity. Participants were not deceived in this study as they were informed that they would be participating in a potential insider threat scenario where they might be invited to play the role of an insider. Ethics approval was obtained from the university's ethics committee.

The participants were set up in a computer studio with a two-way mirror, and the researchers observed in the main room (see Fig. 1). Observers could also view the participant's screen in real time. Participants were provided with login credentials and received a verbal and written briefing outlining their instructions and setting the scene of their role in the simulation. A social media account was created to enhance participants' experience of working within the virtual organisation, and the account's visibility was set to private to negate any unintentional impacts for members of the public. Their communications were recorded. Participants received a debriefing statement at the end of the study and an opportunity to ask questions.

2.3 Materials – The Hybrid Computer Simulation Experiment

The organisational context for the simulation was a marketing team within a fictitious fashion company called 'Next Forward', which developed fashion products for young Australian professionals interested in sustainable, locally sourced products. The participant was assigned the public relations and events coordinator role within the company's marketing team. Two coworker characters in the marketing team, both social media coordinators, and all three positions report to the Chief Creative Officer (CCO). Adjacent to the marketing team was the product design and innovation group, which consisted of a director, who reported to the CCO and a junior designer, who reported to the director. The director of product design and innovation was senior to the participant, and the junior designer was subordinate. Notably, the researchers played these characters.



Fig. 1. Photograph of the control room and the simulation viewed from a two-way mirror.

The initial briefing also informed participants that, in the scenario, their long-term friend and former supervisor currently worked as a senior manager for Next Forward's main competitor - ascribed the fictitious title 'YG'. They were informed that this person was aware the participant has recently commenced employment at Next Forward, and they are told they may be approached by this person and offered additional real-world incentives (money) in exchange for interacting with coworkers and extracting and exfiltrating confidential information. They were also advised that these additional monies might be forfeited if Next Forward became aware of their involvement in such activities.

Round 1. The objective of the first round was to set the scene and establish a behavioural baseline before the insider task in Round 2. In this first round, the participant was required to log in to a laptop, access their inbox and read the first email from the CCO. This welcoming message outlined the first task for the participant, who was assigned the PR and events coordinator role. It explained that the participant needed to work collaboratively with one of the social media coordinators to develop ideas for a marketing strategy to launch the company's fashion products. A briefing document providing further information about the company and its products was also sent as an attachment to this initial email. After the participant had time to read through the email and attachment, one of the social media coordinators contacted the participant to discuss ideas for the marketing campaign and sent a video briefing recorded by the CCO, which provided additional information about the company. A meeting between the social media coordinator and the participant was then scheduled, during which the two collaboratively developed ideas for the marketing campaign. The CCO later sent an email requesting a summary of these ideas from the participant. The participant was then interviewed and given a break before the commencement of round 2.

Round 2. Round 2 began when the participant logged into their laptop and accessed another email from the CCO. The email thanked the participant for their work in the

previous round and asked them to independently develop a set of PowerPoint slides addressing the PR and events component of the marketing campaign, linking this to the ideas developed in Round 1. In the email, the participant was encouraged to maintain confidentiality. Shortly after receiving this, the participant was sent an email from the senior manager of a competitor company, referred to as ‘YG’, offering \$50 in return for providing Next Forward’s confidential ‘Spring-Summer’ catalogue. The participant did not know this, but this item was accessible only to the junior product designer and the director of the product design and innovation group. If the participant decided to act as an insider, they needed to work out who had access to this information. Concurrently, they were expected to continue to work on the tasks assigned to them from Next Forward. The participant was then interviewed and given a break before the commencement of round 3.

Round 3. Round 3 followed the same format as the previous round. In the initial email, the CCO thanked the participant for their work in the last round and asked the participant to develop an event plan. A template for the task was attached to the email. The participant subsequently received an email from the competitor company, offering \$50 for confidential information. Notably, if the participant declined the offer in Round 2, the incentive increased to \$100. In this round, the competitor requested Next Forward’s endorsers list, which was only accessible by the two social media coordinators.

The scenario is visualised in Fig. 2. Here, you can see the organisational structure of New Forward and where the participant sits within the organisation. The information held by the different characters is also depicted. The Competitor, YG, is also represented on the right-hand side. The participant was then interviewed and debriefed.

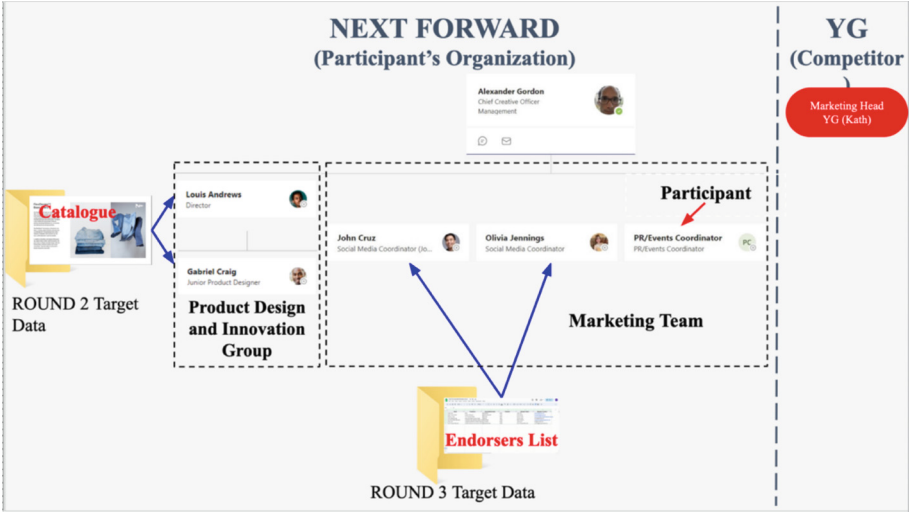


Fig. 2. Organisational Structure, Coworker Status, Target Data and Coworkers with Access.

2.4 Data

We collected all the participants' communications, including emails and IM chats, and analysed them in a separate paper. After each round, the participants were also interviewed about their emotional state and how they were experiencing the scenarios. We conducted a thematic analysis of these interviews, which we present in the results section.

3 Results

This research involved a two-step analysis. The secondary analysis, which involves a linguistic analysis, is reported elsewhere. In this paper, we report the thematic analysis conducted on the interviews to gain insights into the participants' learning experiences.

3.1 Thematic Analysis

The study employed thematic analysis to analyse the transcripts from the interviews. Thematic analysis is a method for identifying, analysing, and reporting patterns (themes) within data, providing a flexible and systematic approach to understanding complex phenomena. Six themes emerged through the analysis of the data. These themes are summarised in Table 1.

Theme 1: Immersive Experience – Felt Real. All the participants noted that the simulation felt very real. They immersed themselves in the role and took the assigned tasks seriously. According to the participants, the organisation seemed authentic, and the characters had personalities that appeared genuine people you would encounter in the workplace. The scenario itself also came across as very realistic and one that could be imagined occurring in their places of work.

Theme 2: Learn About how Insiders Operate. Most participants discussed what they felt they had learnt from the experience. They discussed how they could imagine this occurring in real life, but perhaps more interestingly, they talked about how an insider might go about IP theft. Some thought deeply about the need to persuade and charm others to gain information and be highly covert in their actions. One participant also thought beyond the simulation and discussed how they believed they would meet the character with the IP for coffee to build rapport and have greater success in coxing the information from them.

Theme 3: Importing Personal Ethics into the Simulation. Participants in this research were faced with a potential ethical dilemma. Although it was contained within the boundaries of a game, they nonetheless considered their personal ethics. Some struggled to play a character that did not imbue their personal ethics. This allowed for deep reflection on participants' ethics, and although they understood their behaviours would not have a negative impact, in reality, on others, they were still unable to step beyond their 'real self' to play a deviant character.

Theme 4: Reflected on How they Would Act in Real life. Over a third of participants considered, in light of their experience in the simulation, how they might act in real

Table 1. Themes, example quotes, frequencies and percentages.

	Theme	Example quote	<i>f</i> (%)
1	Immersive experience – felt real	“It felt real. The different interactions with co-workers made this realistic and the goals of the company felt real. I felt guilty for betraying these colleagues”	15 (100%)
2	Learn about how insiders operate	“...in reality, I might have been able to blackmail YG or otherwise use this in the future for the advantage of NF, such as if there was a disagreement over IP”	11 (73%)
3	Importing personal ethics into the simulation	“I blocked the competitor from emailing me. It would have been an ethical violation to receive emails from her [the character asking him to steal IP]”	7 (47%)
4	Reflected on how they would act in real life	After this, I would not act as an insider in the future, it would be a straight no”	6 (40%)
5	Were able to separate the simulation from real life	“I was tempted by the \$100 incentive...I wouldn't do this in real life, but this is a simulation.”	4 (27%)
6	Mirror of real life	“The scenario resembled a situation I had at work...as a product manager on a new feature for a streaming platform and employee left....and later contacted me with an offer of over \$5000 for confidential information”	2 (13%)

life. The simulation brought to life how IP theft might occur in the real world and the possibilities of being approached in their places of work. They acknowledged the temptations and the challenges of wanting to appease a friend but believed they would not succumb to these in reality.

Theme 5: Were Able to Separate the Simulation from Real Life. This theme demonstrated that some participants considered the separation of the computer simulation from real life. When asked about their decisions to play an insider, some felt the need to qualify that although they decided to play this role, it was not a choice they would make in their ‘real’ places of work. They held these views despite the simulation feeling like an authentic experience.

Theme 6: Mirror of Real Life. Two of the participants had personally experienced a similar insider threat scenario at their workplaces. They commented on how realistic the simulation and characters were compared to their real-life experiences.

4 Discussion

This study developed a hybrid computer simulation that can be used to educate employees about malicious insider threats – in particular, IP theft. The main objective of the research was to examine the utility of this hybrid computer simulation method in educating and training employees about malicious IP theft. A secondary aim was to draw from these findings to suggest how these methods might be used to educate and train adults about other types of technology misuse, such as scams, trolling, bullying and sabotage. The results reported here include a thematic analysis of transcripts from interviews with fifteen participants who consented to play the hybrid insider computer simulation.

4.1 Immersive Experience

As highlighted earlier in this paper, immersive experiences play a pivotal role in adult learning by creating realistic and engaging environments where learners can actively apply knowledge and skills. Immersion fosters active participation, allowing adults to learn through doing rather than passive consumption. By creating authentic, contextually relevant experiences, immersive learning environments prepare adults for the complexities of real-world challenges, making them a valuable tool in modern education and training.

Our hybrid simulation allowed us to control the scenario whilst maintaining a safe space for the participants to partake in the experiment (a point we will discuss in more detail later in this paper). All our participants described their experiences as very realistic, and they could fully engage with the experiment. They talked about how they felt emotionally and morally about engaging in and reflecting on the scenario. Two participants reported that the scenario resembled a situation in their workplaces. The ‘realness’ of the scenario helped them gain insights into how an insider might be tempted to engage in IP theft and the potential methods to be successful at these attacks.

4.2 Reflective Learning

Reflection is central to adult learning, particularly within the framework of Mezirow’s (2018) Transformation Learning Theory, which emphasises the role of critical reflection in fostering profound and cognitive change. According to Mezirow, transformative learning occurs when adults critically examine their existing assumptions and beliefs, allowing them to revise their worldviews and develop a deeper understanding of themselves and their environments.

In Mezirow’s Transformation Learning Theory, he discusses the concept of a disorienting dilemma as a pivotal event or experience that disrupts an individual’s worldview, prompting critical reflection and potential transformation. Examples of dilemmas are life events or crises, such as a career change, illness or cultural dislocation – that challenge deeply held beliefs and assumptions. This disruption creates cognitive and emotional discomfort, pushing individuals to question the validity of their perspectives and engage in reflective thinking.

Although the participants were not necessarily presented with a life-changing dilemma – they nonetheless all seemed to agree that it was disorienting and one that

prompted reflection. It appeared to prompt reflections on morals and ethics, how they felt about their role in the scenario, and what this meant for beliefs and potential actions in their lives. Most of our participants (73%) stated they learnt how IP theft insiders might operate, and almost half (40%) reflected on how they might respond in real life in a similar scenario. They discussed how this experience gave them new insights and understandings about insider threats they would take into their real-world lives.

According to Mezirow, ‘self-oriented reflection’ examines one’s experiences, assumptions, and values. This type of reflection requires individuals to scrutinise how their beliefs and past experiences influence their understanding of the world. Some participants in this study (40%) could (unprompted) reflect upon how they would act should they find themselves in a similar workplace situation. Again, although not directly asked, participants reflected on their personal ethics and how this led them to behave in the scenario. The simulation allowed them to consider their morals and beliefs about IP theft that they had not previously thought about. As noted, the researchers did not directly ask participants how they might behave at work after undertaking this experience; however, future research might consider including this as a standard interview question to gain future insights into individuals’ cognitive processing.

Mezirow also considered ‘other-oriented reflection’, which he referred to as involving the perspectives, values, and experiences of others. He highlighted the importance of this outward-focused reflection in helping individuals appreciate diverse viewpoints and challenge ethnocentric or egocentric ways of thinking. In this study, most (73%) participants thought deeply about how the insiders might operate in the real world. Sometimes, this meant thinking about the steps needed to be successful at the attack; however, others felt some understanding about how insiders might feel when confronted with this dilemma and how challenging it might be for someone – especially given the external was a friend. Interestingly, some demonstrated empathy towards insiders.

Research on other types of deviant behaviours has found that role-play simulations can be an effective active learning strategy (e.g., Sonja et al. 2012; Gillespie et al. 2015). For example, Gillespie et al. (2015) found that role-play bullying simulations effectively educated nurses about entering the workplace. However, these are mainly face-to-face role plays, and little work (if any) examines the misuse of technology.

Notably, in this simulation, we built reflection phases to allow participants to reflect on their experiences after each round. This provided a safe space for anyone who might be feeling distressed. We recommend that future researchers include these reflection phases in their simulations.

4.3 Online Spaces – A Safe Space for Learning

Arguably, cyberspace and computer simulations are safe spaces to learn about unethical and immoral behaviours in the real world (Shilton et al. 2022; Whitty et al. 2011; Young and Whitty 2010, 2012). Previous experiments deemed unethical to conduct in face-to-face settings, such as Milgram’s infamous obedience experiment, have been deemed acceptable online (Slater et al. 2006). The reasoning is that the separation between reality and gamespace provides a psychologically safe space to engage in these studies. These virtual spaces can motivate people to act in ways that can be generalised to non-virtual environments that are less safe and easy to control (Young 2010). To illustrate, Blodgett

et al. (2022) developed virtual scenarios simulating racism in healthcare settings to help practitioners better understand, confront and cope with this behaviour in the workplace. As with the bullying studies mentioned in this paper, running similar studies examining these behaviours in face-to-face settings may be ethically challenging.

Relatedly, this research examined the viability of learning about criminal behaviours in hybrid simulation studies. Our research focused on IP theft scenarios; however, it could arguably be applied to other adult learning about criminal, upsetting, and unethical behaviours in the real world, such as fraud, bullying, stalking, and so forth.

4.4 Limitations and Future Work

Several limitations are important to note. The small sample size makes it difficult to generalise the findings. The interview questions might have asked more directly about what the participants learnt from the experience. Nonetheless, this is the first hybrid simulation of its kind, and we hope that future research can build upon this work.

Organisations might use the hybrid scenario developed here to train and educate their employees about malicious insider threats. The research demonstrates that it holds much promise for transformational education. Researchers might also consider drawing upon this work to develop other types of hybrid simulations to train and educate adults about the impact of other technology misuse behaviours, hoping that this might obviate such behaviours.

4.5 Conclusions

Whilst many organisations develop ‘accidental’ insider programmes in the form of phishing detection, few consider education and training around malicious insider threats (Whitty 2021). This is arguably remiss of organisations, given that they can potentially suffer significant losses from these attacks – which sometimes lead to the downfall of an organisation (Whitty 2021). IP theft can significantly harm an organisation. Training managers to spot insider threat behaviours is ineffective. This is perhaps because managers are given a list of behaviours to look out for, which are difficult to spot and can be ambiguous (Nelson et al. 2019).

The hybrid simulation developed here is based on real-life scenarios (Whitty et al. 2023, 2024a, 2024b). Allowing employees to experience this scenario may improve their ability to recognise the signs of insider threats and help managers consider more effective policies to prevent attacks. Moreover, it may allow employees to think deeply about these behaviours and reflect upon their ethical position so that if they find themselves in such a position, they may be better equipped to deal with and report the incident.

Acknowledgments. This research was supported by a grant funded by the Department of Defence Next Generation Technologies Fund (NGTF) initiative.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

- Almomani, E., Sullivan, J., Saadeh, O., Mustafa, E., Pattison, N., Alinier, G.: Reflective learning conversations model for simulation debriefing: a co-design process and development innovation. *BMC Med. Educ.* **23**, 837 (2023) <https://doi.org/10.1186/s12909-023-04778-0>
- Basyuk, T., Vasyliuk, A., Ushenko, Y., Uhryn, D., Hu, Z., Talakh, M.: Modeling and development of a computer simulator with formation of working scenarios for training operator personnel in the search for objects. *Int. J. Mod. Educ. Comput. Sci.* **4**, 87–112 (2023). <https://doi.org/10.5815/ijmecs.2024.04.07>
- Bell, B.S., Kozlowski, S.W.J.: Active learning: effects of core training design elements on self-regulatory processes, learning, and adaptability. *J. Appl. Psychol.* **93**(2), 296–316 (2008). <https://doi.org/10.1037/0021-9010.93.2.296>
- Bell, A.J., Rogers, M.B., Pearce, J.M.: The insider threat: behavioral indicators and factors influencing likelihood of intervention. *Int. J. Crit. Infrastruct. Protect.* **24**, 166–176 (2019) <https://doi.org/10.1016/j.ijcip.2018.12.001>
- Blodgett, N.P., Howard, V.M., Phillips, B.C., Andolsek, K., Molloy, M.A.: Developing virtual simulations to confront racism and bias in health professions education. *Clin. Simul. Nurs.* **71**, 105–111 (2022). <https://doi.org/10.1016/j.ecns.2022.03.009>
- Cappelli, D., Moore, A., Treciak, R.: *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Pearson Education Inc., Massachusetts (2012)
- Clair, R.: Andragogy: past and present potential. *New Direct. Adult Contin. Educ.* **2024**(184), 7–13 (2024). <https://doi.org/10.1002/ace.20546>
- Clapper, T.C.: Beyond Knowles: what those conducting simulation need to know about adult learning theory. *Clin. Simul. Nurs.* **6**, e7–14 (2010). <https://doi.org/10.1016/j.ecns.2009.07.003>
- Dunphy, P., et al.: Understanding the experience-centeredness of privacy and security technologies. In: *NSPW'14: Proceedings of the 2014 New Security Paradigms Workshop*, pp. 83–94. ACM, New York (2014) <https://doi.org/10.1145/2683467.2683475>
- Gillespie, G.L., Brown, K., Grubb, P., Shay, A., Montoya, K.: Qualitative evaluation of a role play bullying simulation. *J. Nurs. Educ. Pract.* **5**(6), 73–80 (2015). <https://doi.org/10.5430/jnep.v5n6p73>
- Greene, K., Larsen, L.: Virtual andragogy: a new paradigm for serving adult online learners. *Int. J. Digital Soc. (IJDS)* **9**(2), 1376–1381 (2018) <https://doi.org/10.20533/ijds.2040.2570.2018.0169>
- Greitzer, F.L., Moore, A.P., Cappelli, D.M., Andrews, D.H., Carroll, L.A., Hull, T.D.: Combating the insider cyber threat. *IEEE Secur. Priv.* **6**(1), 61–64 (2008). <https://doi.org/10.1109/MSP.2008.8>
- Gudoniene, D., et al.: Hybrid teaching and learning in higher education: a systematic literature review. *Sustainability* **17**(2), 756 (2025). <https://doi.org/10.3390/su17020756>
- Gum, L., Greenhill J., Dix, K.: Clinical simulation in maternity (CSiM): interprofessional learning through simulation team training. *Qual. Saf. Health Care* **19**(5), e19, 1–5 (2010). <https://doi.org/10.1136/qshc.2008.030767>
- Hight, M.P., Fussell, S.G., Kurkchubasche, M.A., Hummell, I.J.: Effectiveness of virtual reality simulations for civilian, ab initio pilot training. *J. Aviat./Aeros. Educ. Res.* **31**(1), 1–17 (2022) <https://doi.org/10.15394/jaaer.2022.1903>
- Kavak, H., Padilla, J.J., Vernon-Bido, D., Diallo, S.Y., Gore, R., Shetty, S.: Simulation for cybersecurity: state of the art and future directions. *J. Cybersecur.*, 1–13 (2021) <https://doi.org/10.1093/cybsec/tyab005>
- Kelleci, O., Aksoy, N.C.: Using game-based virtual classroom simulation in teacher training: user experience research. *Simul. Gaming* **52**(2), 204–225 (2020). <https://doi.org/10.1177/1046878120962152>

- Khando, K., Gao, S., Islam, S.M., Salman, A.: Enhancing employees information security awareness in private and public organisations: a systematic literature review. *Comput. Secur.* **106**, 102267 (2021). <https://doi.org/10.1016/j.cose.2021.102267>
- Knowles, M.S.: Andragogy: adult learning theory in perspective. *Community Coll. Rev.* **5**(3), 9–20 (1978). <https://doi.org/10.1177/009155217800500302>
- Liu, L., De Vel, O., Han, Q.-L., Xiang, Y.: Detecting and preventing cyber insider threats: a survey. *IEEE Commun. Surv. Tutor.* **20**(2), 1397–1417 (2018). <https://doi.org/10.1109/COMST.2018.2800740>
- Mezirow, J.: Transformative Learning Theory. In: Illeris, K. (ed.) *Contemporary Theories of Learning*, pp. 1–15. Routledge, London (2018)
- McCaughey, C.S., Traynor, M.K.: The role of simulation in nurse education. *Nurse Educ. Today* **30**, 827–832 (2010). <https://doi.org/10.1016/j.nedt.2010.03.005>
- McGrath, V.: Reviewing the evidence on how adult students learn: an examination of Knowles' andragogy model. *Irish J. Adult Commun. Educ.*, 99–110 (2009) <https://eric.ed.gov/?id=EJ860562>. Accessed 28 Jan 2025
- Nelson, L.C., Beneda, J.G., McGrath, S.M., Youpa, D.G.: Enhancing supervisor reporting of behaviors of concern. *PERSEREC, OPA Report No.*, pp. 2019–033 (2019) <https://apps.dtic.mil/sti/pdfs/AD1075281.pdf>. Accessed 28 Jan 2025
- Nurse, J.R.C., et al.: A critical reflection on the threat from human insiders – its nature, industry perceptions, and detection approaches. In: Tryfonas, T., Askoxylakis, I. (eds.) *Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22–27, 2014. Proceedings*, pp. 270–281. Springer International Publishing, Cham (2014). https://doi.org/10.1007/978-3-319-07620-1_24
- Prebot, B., Du, Y., Gonzalez, C.: Learning about simulated adversaries from human defenders using interactive cyber-defense games. *J. Cybersecur.* **9**(1), tyad022 (2023) <https://doi.org/10.1093/cybsec/tyad022>
- Sarkar, K.R.: Assessing insider threats to information security using technical, behavioural and organisational measures. *Inf. Secur. Tech. Rep.* **15**(3), 112–133 (2010). <https://doi.org/10.1016/j.istr.2010.11.002>
- Sang, C.: Applications of andragogy in multidisciplinary teaching and learning. *J. Adult Educ.* **39**(2), 25–35 (2010). <https://files.eric.ed.gov/fulltext/EJ930244.pdf>. Accessed 28 Jan 2025
- Shilton, K., Heidenblad, D., Porter, A., Winter, S., Kendig, M.: Role-playing computer ethics: designing and evaluating the privacy by design (PbD) Simulation. *Sci. Eng. Ethics* **26**, 2911–2926 (2022). <https://doi.org/10.1007/s11948-020-00250-0>
- Shin, J., Carley, K.M., Richard Carley, L.: Integrating human factors into agent-based simulation for dynamic phishing susceptibility. In: Thomson, R., Al-khateeb, S., Burger, A., Park, P., Pyke, A.A. (eds.) *Social, Cultural, and Behavioral Modeling: 16th International Conference, SBP-BRiMS 2023, Pittsburgh, PA, USA, September 20–22, 2023, Proceedings*, pp. 169–178. Springer Nature Switzerland, Cham (2023). https://doi.org/10.1007/978-3-031-43129-6_17
- Slater, M., et al.: A virtual reprise of the Stanley Milgram obedience experiments. *PLoS ONE* **1**(1), 1 (2006). <https://doi.org/10.1371/journal.pone.0000039>
- Soilis, N., Bhanji, F., Kinsella, E.A.: Virtual reality simulation for facilitating critical reflection and transformative learning: pedagogical, practical, and ethical considerations. *Adv. Simul.* **9**, 49 (2024). <https://doi.org/10.1186/s41077-024-00319-x>
- Sonja, P., Knauss-Forrester, C., Alsaker, F.D.: Self and other oriented social skills: differential associations with children's mental health and bullying roles. *J. Educ. Res. Online* **4**(1), 99–123 (2012). <https://doi.org/10.25656/01:7053>
- Stancil, S.: So, do reusable assignments really benefit students? *J. Open Educ. Res. High. Educ.* **3**(1), 62–79 (2025). <https://doi.org/10.31274/joerhe.17911>

- Taylor, P.J., et al.: Detecting insider threats through language change. *Law Hum Behav.* **37**(4), 267–275 (2013). <https://doi.org/10.1037/lhb0000032>
- Whitty, M.T.: Developing a conceptual model for insider threat. *J. Manag. Organ.* **27**(5), 911–929 (2021). <https://doi.org/10.1017/jmo.2018.57>
- Whitty, M.T., Mostafa, N., Grobler, M.: Cybersecurity when working from home during COVID-19: considering the human factors. *J. Cybersecur.* **10**(1), tyae001 (2024a). <https://doi.org/10.1093/cybsec/tyae001>
- Whitty, M.T., Ruddy, C., Keatley, D., Butavicius, M., Grobler, M.: The prince of insiders: a multiple pathway approach to understanding IP theft insider attacks. *Inf. Comput. Secur.* **32**(4), 509–522 (2024b). <https://doi.org/10.1108/ICS-11-2023-0210>
- Whitty, M.T., Ruddy, C., Keatley, D.A.: To catch a thief: examining socio-technical variables and developing a pathway framework for IP theft insider attacks. In: Furnell, S., Clarke, N. (eds.) *Human Aspects of Information Security and Assurance: 17th IFIP WG 11.12 International Symposium, HAISA 2023, Kent, UK, July 4–6, 2023, Proceedings*, pp. 377–390. Springer Nature Switzerland, Cham (2023). https://doi.org/10.1007/978-3-031-38530-8_30
- Whitty, M.T., Young, G., Goodings, L.: What I won't do in pixels: examining the limits of taboo violation on MMORPGs. *Comput. Hum. Behav.* **27**, 268–275 (2011). <https://doi.org/10.1016/j.chb.2010.08.004>
- Young, G.: Virtually real emotions and the paradox of fiction: Implications for the use of virtual environments in psychological research. *Philos. Psychol.* **23**(1), 1–21 (2010). <https://doi.org/10.1080/09515080903532274>
- Young, G., Whitty, M.: *Transcending Taboos: A Moral and Psychological Examination of Cyberspace*. Routledge, London (2012) <https://doi.org/10.4324/9780203126769>
- Young, G., Whitty, M.T.: Games without frontiers: on the moral and psychological implications of violating taboos withing multi-player virtual spaces. *Comput. Hum. Behav.* **26**(6), 1228–1236 (2010). <https://doi.org/10.1016/j.chb.2010.03.023>