Shih, JL. et al. (Eds.) (2023). Proceedings of the 31st International Conference on Computers in Education. Asia-Pacific Society for Computers in Education

Collaborate, Design, and Generate Cybercrime Script Tabletop Exercises for Cybersecurity Education

Joshua DWIGHT[a*]
[a]*School of Science, Engineering, & Technology, Royal Melbourne Institute of Technology, Vietnam*
*Joshua.dwight@rmit.edu.vn

Abstract: Cyber incidents are frequent, urgent, and sophisticated, and there is a global shortage of cybersecurity professionals. The demand for cybersecurity graduates is high, and a key priority for universities is improving successful graduate outcomes, employability, and work readiness. This research paper proposes a novel teaching approach to develop the skills and experience of higher education students for cybersecurity roles. The approach synthesizes problem-based learning, work-integrated learning, tabletop exercises, and crime script analysis. The paper presents a theoretical model based on the National Institute of Standards and Technology (NIST) Test, Training, and Exercise (TT&E) methodology and suggests using Generative AI for the development of draft documentation. The Cybercrime Script Tabletop Exercise can be integrated into a cybersecurity curriculum or as a stand-alone workshop. Future research can be conducted to compare, interview, and observe student outcomes such as skill and experience acquisition, work-life awareness, and levels of industry professional involvement.

Keywords: problem-based learning, work-integrated learning, tabletop exercise, crime script analysis, cybersecurity education, generative AI

1. Introduction

Cyber incidents are becoming more frequent, urgent, and sophisticated (Brilingaitė et al., 2017; Zhang et al., 2021; Dwight, 2023), and there is a global shortage of 3.5 million skilled cybersecurity professionals (Angafor et al., 2020; Towhidi & Pridmore, 2023; Lunn et al., 2021). An international Fortinet research report specified that 68% of organizations face a shortage of cybersecurity skills (2023). Cybersecurity training is more important than ever (Chowdhury & Gkioulos, 2022). However, organizations do not have the necessary skill set to defend against sophisticated and continually evolving threats and cybercrimes (Angafor et al., 2020), and security training programs are often poorly developed and received (Reeves et al., 2021). To meet the labor demand, preparing higher education students for the cybersecurity workforce is a crucial priority for many universities, business organizations, and governments.

RQ: How can higher education academics develop and design tabletop exercises for students to develop skills and experience for cybersecurity roles?

This research paper aims to develop a novel teaching approach to develop the skills and experience of higher education students for cybersecurity roles. This paper will start with a literature review providing background and the gaps between cybersecurity education, learning and design paradigms, tabletop exercises, and crime script analysis. Then, this paper presents a theoretical model based on the National Institute of Standards and Technology (NIST) Test, Training, and Exercise (TT&E) methodology. Next, the theoretical model showcased the integrative model and utilized Generative AI for the development of sample

tabletop exercise documentation. Lastly, the paper wraps up with a discussion of the significant themes, limitations, future research, and implications.

2. Literature Review

2.1 Cybersecurity Education

Cyber incidents are prevalent (Brilingaitė et al., 2017; Zhang et al., 2021), and in the industry, there is a global shortage of skilled cybersecurity professionals (Angafor et al., 2020; Towhidi & Pridmore, 2023). Cybersecurity training and education are more important than ever (Chowdhury & Gkioulos, 2022), as is the demand for cybersecurity graduates (McGettrick, 2013). An educated workforce is essential for developing trustworthy systems, but pedagogical teaching issues exist (Schneider, 2013). The education sector is often sluggish to transform and adapt to technologies (Lim et al., 2023). Improving successful graduate outcomes, employability, and work readiness has been a critical priority for many universities (Aprile & Knight, 2020; Kay et al., 2019). Developing cybersecurity education and curriculum can use both problem-solving and skill development types of active learning and design paradigms.

2.2 Problem-Based Learning (PBL)

Problem-based learning (PBL) is an educational approach whereby a problem is the starting point of the learning process (De Graaf & Kolmos, 2003). PBL typically involves eight to ten students working on a scenario with a facilitator to guide the students in a multi-step process (Bate et al., 2013). PBL helps students develop knowledge and skills to solve real problems (Hallinger, 2020). PBL has been successfully used in a variety of higher education disciplines for over 30 years (Clancey, 2020). The benefits of PBL include better industry performance, efficiency, competency, and interaction between students and faculty (Bate et al., 2013). PBL is the most comprehensive documented active learning method used in education today, although dominated by the medical education field (Hallinger, 2020). The emergence of the active learning school of thought has led to increased adoption and blending of PBL with other learning methods (Hallinger, 2020). However, there is very little literature blending PBL and WIL. This study proposes blending PBL with WIL to meet the demands of developing a cybersecurity industry workforce.

2.3 Work-Integrated Learning (WIL)

Work-integrated learning (WIL) is gaining popularity, where significant labor and skill shortages exist (Smith & Worsfold, 2015). WIL is an educational approach incorporating authentic industry practice where students learn and develop by working, networking, and engaging with industry professionals (Kay et al., 2019; Bilsland et al., 2019). The fundamental tenet of WIL is integrating university study and professional practice (Smith & Worsfold, 2015). Work-integrated learning traditionally entails short-term job placements or internships (Kay et al., 2019; Smith & Worsfold, 2015; Bilsland et al., 2019). However, emerging and innovative WIL practices such as co-designed programs (hackathons), active engagement in industry associations, event-based partnerships, use of technology (simulations), regional and global projects, practicums, supervised practice and greater flexibility in duration (brief placements or micro-placements) are gaining traction (Kay et al., 2019; Smith & Worsfold, 2015). Aprile and Knight (2020) note students experienced benefits such as obtaining real-world application of skills, learning through role models, and professional awareness of work life. WIL curriculum design is intended to integrate and apply theory with workplace practices (Smith & Worsfold, 2015). Tabletop exercises could be a helpful design avenue for a range of PBL and WIL opportunities.

2.4 Tabletop Exercises

When offering cybersecurity educational opportunities, tabletop exercises should be considered due to their ability to increase participants' engagement and success in skill acquisition (Chowdhury & Gkioulos, 2022). Tabletop exercises (TTX) are staged events where participants meet in an open forum to discuss actions for a response to a specific real-life scenario or incident (Brilingaitė et al., 2017; Angafor et al., 2020). TTXs are based on communication and information knowledge sharing that may involve multiple roles within government, business, and other organizations (Brilingaitė et al., 2017).

Tabletop exercises can include technical and non-technical activities (Brilingaitė et al., 2017; Angafor et al., 2020). These activities can consist of planning, discussion, and improvement of cyber plans and procedures. Reviewing and improving the skills and abilities of cyber incident response teams. Practicing and improving incident management coordination, prioritization, escalation, communication, and reporting strategies. Reviewing and practicing operational response capabilities such as tools and applications. Practicing and building awareness with different roles and responsibilities during an incident (Angafor et al., 2020). Tabletop exercises can provide several benefits. TTXs offer the acquisition of practical experience, nurture both technical and soft skills, provide opportunities for reflective practice, and are cost-effective to develop and implement (Angafor et al., 2020). Tabletop exercises can be designed in different ways.

Chowdhury and Gkioulos (2022) findings concluded that the involvement of industry professionals should include ease of implementation, time and resource constraints, remote accessibility, and shorter duration. Lunn et al. (2021) performed a study integrating tabletop exercises into the cybersecurity curriculum. The findings specified a significant increase in students' confidence in exploiting software vulnerabilities and implementing network security protocols. Chowdhury and Gkioulos (2022) conducted several exercises with different participants from industry and higher education students. Lunn et al. (2021) and (Chowdhury & Gkioulos, 2022) alluded to work-integrated learning but did not focus on the WIL theory and its connection to cybersecurity education and tabletop exercises. This paper proposes using crime script analysis as the basis for the tabletop design.

2.5 Crime Script Analysis

Introduced by Cornish (1994), crime scripts are models that describe predictable and sequential criminal actions, locations, and roles (Dehghanniri & Borrion, 2021). Crime script analysis (CSA) is an investigation profiling method that breaks down the actions of a criminal into stages to understand the behaviors, feelings, and decisions associated with the offense (Bada & Nurse, 2021). Cornish (1994) established seven stages that included preparation, entry, pre-conditions, instrumentals, doing, post-conditions, and exit. Later academic works have created similar truncated versions of the initial four stages, such as preparation, pre-activity, activity, and post-activity, that incorporate the other elements (Bada & Nurse, 2021; Bodker et al., 2022; Leppänen et al., 2020). Then the CSA model identifies areas of disruption by appropriate stakeholders (Cornish, 1994). This model provides a great outline to identify cybercriminal behaviors and attacks and allows cybersecurity professionals and students to recognize where and when cybersecurity measures can be used to mitigate cyber offenses.

Clancey's teaching pedagogy was influenced by problem-based learning and the integration of CSA into that PBL teaching pedagogy (Clancey, 2020). Clancey noted this pedagogy encouraged deeper thinking about motivations and root causes beyond crime risk factors and opportunities for criminal offenses (2020). See Table 1 for a summary of the paradigms and benefits. However, there was minimal literature applying and connecting these models.

Each of these models exhibits elements of active learning, although not expressed explicitly in the academic literature. Active learning is the activities designed to engage students in their learning with discussion, problem-solving, and or learning from each other (Nguyen et al., 2021).

Table 1. *Summary of paradigms and benefits*

Paradigm	Summary	Learning Benefits
Problem-based learning (PBL)	Industry problem scenario Multi-step/procedural Active learning	Industry preparation Skill and knowledge competency
Work-integrated learning (WIL)	Integration of university study and industry practice Active learning	Practical skill acquisition and application Work-life awareness Industry preparation
Tabletop exercise (TTX)	Industry problem scenario Multi-step/procedural Active learning	Practical skill acquisition Reflective practice Cost-effective
Crime script analysis (CSA)	Industry problem scenario Multi-step/procedural Active learning	Profiling cybercriminals Skill and knowledge competency

2.6 Literature Gaps

Even though active learning has seen positive results, STEM courses have low adoption rates and still predominately focus on lecturing (Nguyen et al., 2021). So it is imperative to try out different active learning techniques to nurture active learning. There are two literature gaps between PBL, WIL, tabletop exercises, and CSA. First, crime script analysis is used primarily as an investigative, analytical method and has not been applied as a mode of learning. Thus, it has not been applied in the cyber security context with PBL, WIL, or tabletop exercises. Secondly, there has been very little application between WIL and tabletop exercises. Lunn et al. (2021) and Chowdhury and Gkioulos (2022) alluded to using industry professionals for different aspects of tabletop exercise development but did not explicitly identify and apply the WIL approach. This paper aims to create a novel approach integrating these areas to better prepare and develop university students for professional cybersecurity roles to fill the skills gap.

3. Methodology

The National Institute of Standards and Technology (NIST) Test, Training, and Exercise (TT&E) methodology was used to help design a tabletop exercise integrated with PBL, WIL, and CSA for this paper. The NIST tabletop exercise methodology consists of four phases. The phases are design, development, conduct, and evaluation (Grance et al., 2006). The design phase establishes the topics, scope, objectives, participants, and logistics of the exercise. The development phase is the formation of all documentation and the establishment of tools necessary to conduct the exercise. These can be materials such as manuals, evaluation criteria, simulations, and gamification software. The conduct phase performs the exercise based on the design and development. The evaluation phase captures the lessons learned, discussions, and reflections from the exercise (Grance et al., 2006).

4. Cybercrime Script Tabletop Theoretical Framework

4.1 Design Phase

The design phase establishes the topic, scope, objectives, and participants of the exercise (Grance et al., 2006). The topic proposed for this approach is cybercrime incidents and mitigation response using CSA. Problem-based learning (PBL) can be applied design of the tabletop exercise. PBL starts with a problem-solving scenario (De Graaf & Kolmos, 2003). For this paper, cybercrimes are the problem and topic for the tabletop exercise. The scope of the TTX exercise will focus predominately on the tactical level roles and responsibilities. The time scope is limited to 1-3 hours. The delivery scope should be virtual or hybrid to accommodate the industry professional. The objective of the TTX is to identify and analyze cybercrimes based on the CSA. This paper proposes groups of 8-10 student participants per team with facilitators from both academia and industry. Each participant will be provided with a real-world role and responsibility based on input from an industry professional.

Work-integrated learning (WIL) can be applied through the academic lecturer and industry professional working together to design the specific cybercrime, threat, and or attack as the topic, scope, and objective based on a real-world scenario. Some examples are account takeover, credit card fraud, credit card testing, gift card fraud, subscription fraud, triangulation fraud, social engineering, credential stuffing, romance scams, 1st person misuse, identity theft, denial-of-service, phishing, ransomware, advanced persistent threats (Dwight, 2023; Han et al., 2023). The industry professional can also act as a facilitator of the exercise. See Table 2 for the cybercrime tabletop exercise design outline.

Table 2. *Cybercrime Tabletop Design Outline*

TTX	Description	Model Synthesis
Topic:	Cybercrime incident response and mitigation	PBL, WIL, CSA
Scope:	Participant level: Tactical level Duration: 1-3 hours Delivery: Virtual/blended	WIL
Objectives:	Identify and analyze cybercriminal actions and behaviors Identify and analyze cybersecurity mitigations and strategies Create a cybercrime script document based on the exercise Discuss the results of the exercise	PBL, WIL, CSA
Participants:	Groups of 8-10 Students Two facilitators (one academic and one industry professional)	WIL

4.2 Development Phase

The development phase identifies all the documentation and tools necessary to conduct the exercise. This includes a briefing, facilitator guide, participant guide, and lessons learned report (Grance et al., 2006). The briefing consists of the agenda and logistics information. The facilitator guide consists of the purpose, scope, objectives, scenario, and list of questions. The participant guide consists of the shortened version of the facilitator guide without the list of questions. The lessons learned report contains evaluation criteria and reflective practice (Grance et al., 2006).

There are numerous tools to support the development and delivery of the exercise. The development of the documentation can use Generative AI. Generative AI presents an

opportunity to innovate and transform learning as higher education has been sluggish and underwhelming (Lim et al., 2023). Generative AI tools allow new frontiers in the way we learn, interact, and work with each other (Lim et al., 2023). Educational learning opportunities should use Generative AI to encourage transformation in the higher education realm. For this paper, we propose using Generative AI for the development of draft documentation and then revising it with input from the academic and industry partner.

For the delivery of the tabletop exercise, this paper proposes utilizing video conferencing software and a web-based interface (Zhou et al., 2015) to host the activity virtually or in a blended learning environment. Additionally, web-based interfaces can have meaningful effects on the scenario presentation and delivery (Zhou et al., 2015). This helps afford flexibility and cost-effectiveness for industry participation and academics (Chowdhury & Gkioulos, 2022).

4.3 Conducting Phase

The conduct phase is where the designed and developed exercise is executed with the relevant learners, processes, and systems. The facilitators start with the briefing and provide learners with the participant guide. The facilitator will procedurally go through the cybercrime script analysis stages of preparation, pre-activity, activity, and post-activity. At each stage, the learners will discuss and choose appropriate cybersecurity mitigation strategies. Each group of learners will fill out the CSA procedures and mitigations. Then a comparison of the results with other groups should occur in the evaluation phase.

4.4 Evaluation Phase

The evaluation phase captures the lessons learned, discussions, and reflections from the exercise. The learners will present their cybercrime scripts to each other and the facilitators. Then discuss the practicalities of the security measures with the facilitators. The industry professional can provide context about their experiences with the specific cyber-attack. See Figure 1 for the theoretical integrative approach. See Figure 2 for a sample draft briefing for a ransomware scenario, sample draft facilitator guide, participant guide, and after action guides created with the Generative AI technology Notion AI.

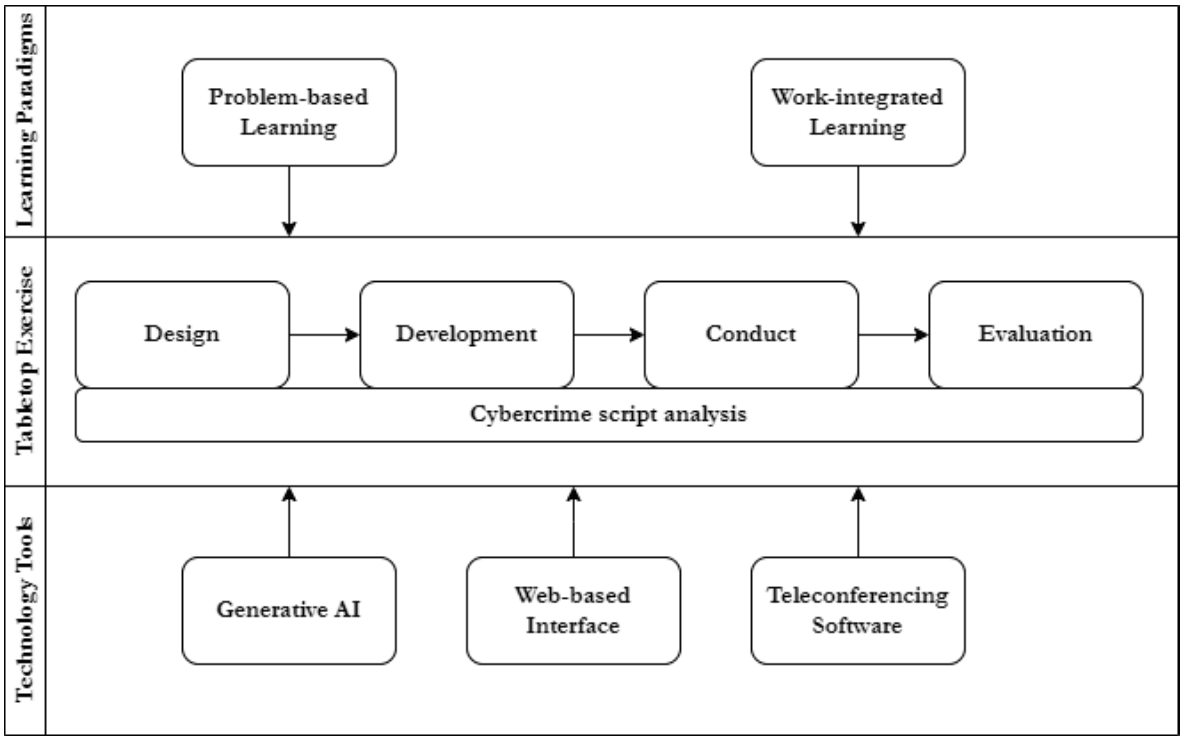

Figure 1. Cybercrime Script Tabletop Exercise Approach.

Crime Script: Ransomware Attack on an Ecommerce Company

On a quiet Monday morning, the IT department of an ecommerce company received an odd message on their computers. The message read "Your files have been encrypted. Pay $10 million dollars in bitcoin to retrieve them." The IT department was confused and assumed it was a prank. But soon they realized that their entire system had been compromised by a ransomware attack.

The attackers had infiltrated the company's network through a phishing email that was sent to an unsuspecting employee. Once the employee clicked on the link in the email, the ransomware virus was downloaded onto the company's network. The virus quickly spread throughout the system, encrypting all of the company's files and rendering their data inaccessible.

The attackers demanded a ransom of $10 million dollars in bitcoin in exchange for the decryption key needed to unlock the company's files. The company was forced to shut down their website and all online sales until the issue could be resolved. The IT department worked tirelessly to try and recover the data, but all their efforts were in vain.

The company had no choice but to pay the ransom, as they were losing millions of dollars every day their systems were down. The payment was made and the attackers provided the decryption key. The company was able to retrieve their data, but not without significant financial and reputational damage.

The incident was a wake-up call to the company and other ecommerce businesses, reminding them of the importance of cybersecurity measures and the need to stay vigilant against potential threats. The company took steps to improve their security protocols, including conducting regular security audits, educating employees on how to recognize phishing emails, and implementing multi-factor authentication.

Despite their efforts, the company's reputation took a hit and they lost customers due to the prolonged outage. The incident also attracted negative media attention and raised concerns among stakeholders about the company's ability to protect customer data.

In the aftermath of the attack, the company worked to repair its reputation and regain the trust of its customers. They offered compensation to affected customers and implemented additional security measures such as encryption and data backups. The company also engaged with cybersecurity experts to conduct a thorough investigation of the incident and identify ways to prevent future attacks.

While the company was able to recover from the attack, the incident highlighted the devastating impact that ransomware attacks can have on businesses. It also underscored the need for companies to prioritize cybersecurity and take proactive steps to protect their data and customers.

TTX Facilitator Guide

This facilitator guide is based on the National Institute of Standards and Technology (NIST) Special Publication 800-84, "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities." The purpose of this guide is to provide facilitators with the necessary information to conduct a tabletop exercise (TTX) for ransomware incidents.

Introduction

The objective of a TTX is to test the organization's response plan for a ransomware incident. The TTX is designed to simulate a ransomware attack and evaluate the organization's response to the incident. It is important to conduct a TTX on a regular basis to identify gaps in the response plan and to improve the overall effectiveness of the plan.

Preparing for the TTX

Before conducting a TTX, the facilitator should identify the scope of the exercise, define the objectives, and identify the participants. The facilitator should also create a scenario that simulates a ransomware incident, including the initial infection vector, the impact on the organization, and the response actions required.

Conducting the TTX

During the TTX, the facilitator should guide the participants through the scenario, providing them with information as needed. The facilitator should also ensure that the participants adhere to the response plan and identify any gaps in the plan. The TTX should be conducted in a realistic and controlled manner, simulating the stress and pressure of a real ransomware incident.

Evaluating the TTX

After the TTX, the facilitator should conduct a debriefing session with the participants. The debriefing session should identify any issues or gaps in the response plan and discuss ways to improve the plan. The facilitator should also document any lessons learned and update the response plan accordingly.

Conclusion

Conducting a TTX is an important part of an organization's overall ransomware incident response plan. It allows the organization to identify gaps in the plan and improve the overall effectiveness of the plan. This facilitator guide provides the necessary information to conduct a TTX for ransomware incidents based on NIST Special Publication 800-84.

TTX Participant Guide

This participant guide has been created to provide instructions to participants of the Tabletop Exercise (TTX) on how to respond to a ransomware attack. The guide is based on the guidelines provided in the National Institute of Standards and Technology (NIST) Special Publication 800-84, "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities".

Introduction

Ransomware has become a significant threat to organizations as it can cause significant disruptions to business operations and result in financial losses. It is essential for organizations to be prepared to respond to a ransomware attack effectively. A TTX is an excellent opportunity to test the organization's incident response capabilities and identify areas for improvement.

Objectives

The objectives of this TTX are as follows:

1. Identify and analyze cybercriminal actions and behaviors
2. Identify and analyze cybersecurity mitigations and strategies
3. Create a cybercrime script document based on the exercise
4. Discuss and reflect on the results of the exercise

Scenario

The TTX will simulate a ransomware attack on the organization's network. The attack will start with an email phishing campaign, which will result in the installation of ransomware on several endpoints. The ransomware will then spread throughout the network, encrypting files and demanding a ransom payment in exchange for the decryption key.

Roles and Responsibilities

The following roles and responsibilities have been assigned to the participants:

Incident Response Team

The incident response team is responsible for identifying and containing the ransomware attack. The team will coordinate with other teams to ensure that the attack is contained and the impact on the organization's operations is minimized.

TTX After Action guide

This document serves as an after-action guide for ransomware attacks based on the guidelines provided in NIST Special Publication 800-84. The purpose of this guide is to assist organizations in responding to ransomware attacks and to provide recommendations for improving their security posture.

Summary of the Attack

[Provide a brief summary of the ransomware attack, including the date and time of the attack, the systems and data affected, and the impact on business operations.]

Initial Response

[Describe the organization's initial response to the attack, including who was notified, the actions taken to contain the attack, and any challenges encountered during the response.]

Recovery and Restoration

[Detail the steps taken to recover and restore the affected systems and data, including any external resources used, such as cybersecurity consultants or law enforcement.]

Analysis and Assessment

[Provide an cybercrime script analysis of the attack, including the type of ransomware used, the attack vector, and any vulnerabilities exploited. Also, describe the impact of the attack on the organization's business operations, reputation, and financial status. Finally, assess the effectiveness of the organization's security controls.

Lessons Learned

[Identify the lessons learned from the attack, including any improvements that can be made to the organization's security posture, incident response plan, or employee training programs.]

Recommendations

[Provide recommendations for other organizations based on the lessons learned from this attack. These recommendations may include improving security controls, updating incident response plans, or increasing employee training.]

Figure 2. Sample Briefing, Facilitator, Participant, After Action Guides.

Note. Sample draft text generated using NotionAI. (2023, May). Prompt: "Write a crime script about ransomware at an ecommerce company." "Write a ransomware facilitator guide based on https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf". Prompt: "Write a ransomware participant guide based on https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf". Prompt: "Write a ransomware after action report based on https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf". Then the draft text was adapted by the researcher.

5. Discussion

The aim of this research paper is to develop a novel teaching approach to develop the skills and experience of higher education students for cybersecurity roles. The gaps in the literature showcased active learning methods but did not map these methods to address the cybersecurity skills gap. The novel approach presented in this paper synthesizes PBL, WIL,

TTX, and cybercrime script analysis to deliver a cost-effective collaborative skill development model.

5.1 Cybersecurity Education

Cybercrimes, threats, and attacks such as social engineering, fraud, and identity theft are sophisticated and continually evolving (Dwight, 2023; Han et al., 2023). Educators will need to stay abreast of the current threats to adapt the cybercrime script tabletop exercises for learners. This allows for many opportunities to continually update the problem and cybercrime scripts for up-to-date learning for higher education students. Educators should network and discuss current cyber threat trends with industry professionals. Industry professionals can help in any phase of the cybercrime script TTX approach including development, design, delivery, and evaluation.

The Cybercrime Script TTX can be integrated into a cybersecurity curriculum or as a stand-alone class session or workshop. However, this exercise should not be the sole active learning activity for an educator and student. This activity should complement other active learning activities such as internships, hackathons, labs, case studies, and others (Kay et al., 2019; Smith & Worsfold, 2015; Bilsland et al., 2019).

Using Generative AI can help with cyber education development. However, the technology is still in its infancy, and many people are wary about adopting the technology (Lim et al., 2023). This brief research used the technology to create rough drafts of the tabletop exercises. The ability of the Generative AI was not comprehensive, and academics will need to review and adapt the output. Additionally, gamification (Angafor et al., 2020), mixed reality (Shaytura et al, 2021), and other technologies can be integrated, used, and tested in any part of the TTX design, development, delivery, and evaluation process.

5.2 Industry Collaboration (WIL)

The level of involvement of industry professionals can be time-consuming and costly. This paper suggests minimizing the effort on the industry professional while providing an advantageous opportunity for the learners to potentially gain skills and interact with an industry professional in a real-world scenario. Chowdhury and Gkioulos (2022) Specified industry professionals preferred easy, cost-effective, and short-term activities. The level of involvement will ultimately depend on the time and resources available to industry professionals and academics. The more exposure the students have to the industry, the better they will be prepared for the real world.

5.3 Limitations

There may be some limitations to the breadth of the paper. The extent to which the study's findings may be generalized and applied to other situations must be left to the reader's judgment. The scope of this paper was limited to designing a small, cost-effective event-based method that incorporated PBL, WIL, TTX, and CSA. All the technology and process nuances and variances associated with these paradigms may not be reviewed, evaluated, and discussed.

6. Contributions and Future Research

This cybercrime script tabletop exercise contributes to the body of knowledge with a novel approach to developing cybersecurity university students. This research paper provides a way to develop the skills and experience of higher education students for cybersecurity roles through the integration of active learning methods with The National Institute of Standards and Technology (NIST) Test, Training, and Exercise (TT&E) methodology (Grance et al., 2006).

Additionally, students can experience a real-world training method while interacting with an industry professional.

Second, this approach provides a way for industry professionals to get more involved with the development of university students. This model is especially useful to industry professionals who have limited time and resources to devote to students but want to contribute to student development and recruitment.

This paper serves as a starting point to apply the cybercrime script tabletop exercises in cybersecurity teaching practice. The next phase of this research can apply quantitative and qualitative methods to compare, interview, and observe student outcomes such as skill and experience acquisition, work-life awareness, and levels of industry professional involvement. Future studies can evaluate the differences between exercises with and without an industry facilitator, perceptions of students, and perceptions of industry professionals. Other research can investigate variations of this method, such as students going onsite to observe and participate in industry tabletop exercises.

7. Conclusion

Cyber incidents continue to grow in sophistication and urgency, and there is a shortage of capable cybersecurity professionals. This paper contributes to the knowledge base by providing a theoretical teaching approach to integrate active learning methods of problem-based learning (PBL), work-integrated learning (WIL), tabletop exercises (TTX), and crime script analysis (CSA) methods into The National Institute of Standards and Technology (NIST) Test, Training, and Exercise (TT&E) Event methodology to help bridge the cybersecurity industry skills gap. Future research can be conducted to compare, interview, and observe student outcomes such as skill and experience acquisition, work-life awareness, and levels of industry professional involvement.

Acknowledgements

The author would like to thank his family, the ICTDSE2023, ICCE2023, and the Royal Melbourne Institute of Technology for their support.

References

Angafor, G. N., Yevseyeva, I., & He, Y. (2020, October). Bridging the cyber security skills gap: Using tabletop exercises to solve the CSSG crisis. In *Joint International Conference on Serious Games* (pp. 117-131). Cham: Springer International Publishing.

Aprile, K. T., & Knight, B. A. (2020). The WIL to learn: Students' perspectives on the impact of work-integrated learning placements on their professional readiness. *Higher Education Research & Development*, *39*(5), 869-882.

Bada, M., & Nurse, J. R. (2021, June). Profiling the cybercriminal: a systematic review of research. In *2021 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1-8). IEEE.

Bate, E., Hommes, J., Duvivier, R., & Taylor, D. C. (2013). Problem-based learning (PBL): Getting the most out of your students–Their roles and responsibilities: AMEE Guide No. 84. *Medical teacher*.

Bilsland, C., Carter, L., & Wood, L. N. (2019). Work integrated learning internships in transnational education: Alumni perspectives from Vietnam. *Education+ Training*, *61*(3), 359-373.

Bodker, A., Connolly, P., Sing, O., Hutchins, B., Townsley, M., & Drew, J. (2022). Card-not-present fraud: using crime scripts to inform crime prevention initiatives. *Security Journal*, 1-19.

Brilingaitė, A., Bukauskas, L., Krinickij, V., & Kutka, E. (2017, October). Environment for cybersecurity tabletop exercises. In *ECGBL 2017 11th European Conference on Game-Based Learning* (pp. 47-55). Academic Conferences and publishing limited.

Clancey, G. (2020). Teaching crime prevention and community safety. *Scholarship of Teaching and Learning in Criminology*, 59-85.

Chowdhury, N., & Gkioulos, V. (2022, September). A Framework for Developing Tabletop

Cybersecurity Exercises. In *European Symposium on Research in Computer Security* (pp. 116-133). Cham: Springer International Publishing.
Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime prevention studies*, *3*(1), 151-196.
De Graaf, E., & Kolmos, A. (2003). Characteristics of problem-based learning. *International journal of engineering education*, *19*(5), 657-662.
Dehghanniri, H., & Borrion, H. (2021). Crime scripting: A systematic review. *European Journal of Criminology*, *18*(4), 504-525.
Dwight, J. (2023). Ecommerce Fraud Incident Response: A Grounded Theory Study. *Interdisciplinary Journal of Information, Knowledge, and Management*, *18*, 173-202.
Fortinet. (2023). 2023 Cybersecurity Skills Gap Report. Retrieved from https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf
Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., & Good, T. (2006). Guide to test, training, and exercise programs for IT plans and capabilities.
Hallinger, P. (2020). Mapping continuity and change in the intellectual structure of the knowledge base on problem-based learning, 1974–2019: A systematic review. *British Educational Research Journal*, *46*(6), 1423-1444.
Han, K., Choi, J. H., Choi, Y., Lee, G. M., & Whinston, A. B. (2023). Security defense against long-term and stealthy cyberattacks. *Decision Support Systems*, *166*, 113912.
Kay, J., Ferns, S., Russell, L., Smith, J., & Winchester-Seeto, T. (2019). The Emerging Future: Innovative Models of Work-Integrated Learning. *International Journal of Work-Integrated Learning*, *20*(4), 401-413.
Leppänen, A., Toiviainen, T., & Kankaanranta, T. (2020). From a vulnerability search to a criminal case: script analysis of an SQL injection attack. *International Journal of Cyber Criminology*, *14*(1), 63-80.
Lim, W. M., Gunasekara, A., Pallant, J. L., Pallant, J. I., & Pechenkina, E. (2023). Generative AI and the future of education: Ragnarök or reformation? A paradoxical perspective from management educators. *The International Journal of Management Education*, *21*(2), 100790.
Lunn, S., Ross, M., & Liu, J. (2021, December). Cybersecurity Integration: Deploying Critical Infrastructure Security and Resilience Topics into the Undergraduate Curriculum. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 866-871). IEEE.
McGettrick, A. (2013). Toward effective cybersecurity education. *IEEE Security & Privacy*, *11*(6), 66-68.
Nguyen, K. A., Borrego, M., Finelli, C. J., DeMonbrun, M., Crockett, C., Tharayil, S., ... & Rosenberg, R. (2021). Instructor strategies to aid implementation of active learning: a systematic literature review. *International Journal of STEM Education*, *8*, 1-18.
Reeves, A., Calic, D., & Delfabbro, P. (2021). “Get a red-hot poker and open up my eyes, it's so boring” 1: Employee perceptions of cybersecurity training. *Computers & security*, *106*, 102281.
Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security & Privacy*, *11*(4), 3-4.
Shaytura, S., Olenev, L., Nedelkin, A., Ordov, K., Minitaeva, A., & Guzhina, G. (2021, November). Mixed reality in education and science. In *2021 3rd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA)* (pp. 667-673). IEEE.
Smith, C., & Worsfold, K. (2015). Unpacking the learning–work nexus:‘priming’as lever for high-quality learning outcomes in work-integrated learning curricula. *Studies in Higher Education*, *40*(1), 22-42.
Towhidi, G., & Pridmore, J. (2023). Aligning Cybersecurity in Higher Education with Industry Needs. *Journal of Information Systems Education*, *34*(1), 70-83.
Zhang, Z., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management & Data Systems*, *121*(3), 613-636.
Zhou, B., Sun, G., Zhang, X., Xu, J., Lai, J., Du, X., ... & Sakurada, Y. (2015). Development of web-based tabletop emergency earthquake exercise system. *Journal of Disaster Research*, *10*(2), 217-224.