Kepes
http://scholopress.com/kepes-journal

2023 Volume 21 Issue 3 pp. 459-469

Tabletop Exercise in Cybersecurity Incidence Response Education: A Systematic Review

***Omega Sarjiyus [1], Yusufu Gambo [1], Yakubu Atomsa [2]**

[1]Department of Computer Science, Adamawa State University, Mubi, Adamawa State, Nigeria
[2]Computer Science Department, Federal University Kashere, Gombe State, Nigeria

Abstract

The increasing challenges in cybersecurity breaches, the scarcity of qualified cyber incident response (CSIR) professionals, and the continuously altering environment due to cyber threats represent a huge issue for the security industry. Consequently, training providers are always looking for innovative answers to the numerous security issues that currently exists. Both the public and private sectors concur those comprehensive cybersecurity measures, which should include training for workers, must be put into place. Many organizations are now providing their employees and cybersecurity incident response teams (CSIRTs) with cutting-edge training to ensure that they can detect and respond to security breaches in the event that they occur. Tabletop exercises (TTXs) can play a critical role in CSIR training and found to be useful across organizations, however, there is a scarcity of studies explicitly focused on TTX for cybersecurity education which can provide insights and the need for further investigations. This research used systematic review to assessed existing TTX and detailed how they are used in cybersecurity education. It was found that TTX can enhances CSIRTs' awareness, understanding, and preparation, as well as strategic decision-making, allowing them to be better prepared for security crises. Although research on using TTX for cybersecurity education is expanding, this study recommends an urgent need for academic institutions and technical organizations to teach students and employees how to develop and demonstrate technical and non-technical skills. These skills are crucial as it is frequently found to be lacking across organizations. In addition, TTX should be used to supplement traditional methods such as classroom lectures by giving opportunities for practical learning and practice-based approaches to solving real-world problems. This study suggested further research works which can be explore to provide knowledge around TTX for cybersecurity education to support organizational business continuity.

Keywords: Cybersecurity, Cybersecurity training, Incident response, Tabletop exercises, Cybersecurity expert

1. Introduction

Cybersecurity protects internet-connected devices and services against cyber-criminals like hackers and spammers. Organizations use this method to prevent phishing, ransomware, identity theft, data breaches, and financial losses (Sabillon, 2020; Sharif & Ameen, 2020). Although cybersecurity elements are geared to strike first, most specialists are more concerned with discovering the most effective technique to defend all assets, from computers and smart devices to networks and databases from assaults (Gafic, Tjoa, Kieseberg, Hellwig, & Quirchmayr, 2022; Lymn & Raffety, 2021). Cyber-exercises are some tactics for defending against cyber-attacks that have recently gained popularity as a tool for security training, awareness-building, and incident

*Corresponding author

DOI https://doi.org/10.5281/zenodo.7936583#105

response testing (Gafic *et al.,* 2022; Angafor, Yevseyeva & He, 2020; Ulmanová, 2021; Sharkov, Vykopal & Čeleda, 2021). Cyber exercises can enhance employees' knowledge and provide opportunities for training and preparedness against attack. Previous studies show that cybersecurity education is gaining interest among stakeholders. For example, Švábenský et al. (2020) systematically examined 70 articles focused on cybersecurity education. The findings offer insights into the field and a synthesis of current trends and suggestions for future research. In another related study, Angafor et al., (2020) systematically investigated 102 pieces of literature focused on Tabletop-based serious games in CSIR. The findings recommend building TTX to teach and exhibit technical and non-technical skills for CSIR teams and for teaching and learning process. Similarly, Angafor et al. (2020) examined 19 articles dealing with the cyber-skills gap (CSSG) organizations struggle to fill due to a lack of cyber security skills. The finding concluded that there is an urgent need to develop approaches for providing cybersecurity education to meet the global demand. However, these related studies focused on general concepts of TTXs and how they are used across organization. There is a scarcity of studies that explicitly focusing on TTX for cybersecurity education to gain insights and provides directions for further studies. In response to the call by the previous studies, this research systematically reviews the literature on TTX for cybersecurity education. This systematic review discovers, evaluates, and analyzes relevant papers for a research question, topic, or phenomenon and provides guidelines for systematic reviews. It also proposes a search technique, inclusion/exclusion criteria for primary sources, quality criteria used to evaluate each resource, and significant conclusions (Sharif & Amen, 2020; Angafor et al., 2020; Moher, 2009; Moneer, Sean, & Atif, 2021).

The remainder of the paper is organized as follows: The study's background is outlined in Section 2. The research methodology that includes the search strategy, and the standards for selecting the material for the study are covered in Section 3. The results of the research process that addressed research questions are discussed in Section 4. The summary of some gaps and suggestions for additional research are presented in Section 5, and conclusion is discussed in section 6.

2. Background

2.1 Cybersecurity Exercise

Cybersecurity exercise is an activity that improves workforce readiness to combat cyber threats. Today, there are no clear boundaries between the concepts of cybersecurity training, cyber drills, and cyber polygons. Historically, cybersecurity exercises were conducted using paper, command, and staff. The purpose of these events, which brought together representatives from several departments, was to recognize unique abilities. Today, cybersecurity exercises are mostly used to train teamwork (Gafic et al., 2022; Ulmanová, 2021; Sharkov et al., 2021).

Cyber-exercise must precede cyber-resilience development; an organization's ability to respond appropriately to any event is closely connected to the level of preparation it puts into its emergency preparedness process, which includes drills and training for its staff. Businesses must often execute drills on their business continuity plans to ensure their continued existence, making drills a crucial part of corporate resilience and adaptability. To enhance system resilience and prepare for a cyber-threat, employees must be routinely educated to react to threats and communicate under pressure (CISA, 2021, Bahuguna et al., 2019). Exercise participants apply knowledge in practical settings using recognized methodologies and instruments to understand a certain occurrence (Sabillon, 2022; ENISA, 2021; Dewar, 2018). Over the last decade, various cyber exercises have arisen (Leitner et al., 2021); and strive to accomplish several objectives (e.g., to build competencies, assess competencies, etc.). Exercises in cybersecurity can be organized and planned in various ways (CISA, 2021). Cybersecurity exercises, also known as cyber defense exercises (CDX) (Leitner *et al.,* 2021, Kim *et al.,* 2019) are frequently used in organizations to educate and prepared employees against cyber threats.

There are two general categories of cybersecurity exercises across literature: operational and theoretical (discussion-based learning) (Lynn & Raffety, 2021; Angafor et al., 2020). Operational-Based learning exercises are centered on operations, such as drills, functions, and full-scale functional exercises, which are both resource expensive and high stress. In most cases, participants must move to a virtual location in real-time while utilizing real equipment (Sabillon, 2022; Sharif & Ameen, 2020). While theoretical is based on discussions, such as seminars, workshops, games, Tabletop, etc., it brings participants together in low-stress environments to talk about their existing plans, processes, and response capabilities, typically about a hypothetical scenario (Angafor et al., 2020; Moneer et al., 2021). Table-top exercises are a systematic approach for conducting cyber exercises with participants from various domains, and it was found to be frequently used to support cybersecurity education (Angafor et al., 2020; Denning *et al.,* 2013; Rashid *et al.,* 2019).

2.2 Tabletop Exercise

A Tabletop exercise is a facilitated discussion of a scripted situation where important employees are assigned emergency management tasks. Tabletop exercises examine existing crisis response plans and procedures in a safe environment to detection and enhance procedural weakness (CISA, 2021; Hobbs *et al.,* 2016; RTT, 2021). Tabletop exercises are done in class without special equipment. The facilitator introduces the scenario and starts a conversation. According to the National Institute of Standards and Technology (NIST), a Tabletop exercise should have four components: develop the scenario and participant guides, conduct the exercise, and then evaluate through debriefing and identifying lessons learned (Uenuma & Strukturer, 2018). These exercises increase problem-solving, communication, teamwork, and business processes. These abilities prepare future professionals to work on cybersecurity incident response teams (Švábenský et al., 2020; Kim et al., 2019).

Tabletop exercises focus on the verbal recounting of an experience. Participants are frequently grouped in a single area, sometimes in the same conference room, to imitate response who need to communicate and coordinate. After participants are allocated roles in the emergency response system being trained, these exercises begin with a simulated incident narrative. Participants respond to event demands by explaining the steps they would take since contacts with other response or agencies are minimized. Exercise managers (controllers) perform the exercise protocol and evaluate participant's responses, sometimes varying events, to test exercise objectives (Sharif & Ameen, 2020; Gafic et al., 2022; Moneer et al., 2021). Evaluation and self-critique might be done after or during these exercises and is beneficial for validating methods and identifying shortcomings. Tabletop exercises are the least formal sort and tend to achieve relatively generic evaluations but are cost-effective and valuable when new procedures are incorporated into existing response systems or when previously uncontrolled hazards are detected (Sabillon, 2020; Angafor et al., 2020; Julius, 2014).

2.3 Tabletop Exercise Products for Cybersecurity Training

This section summarizes the TTX products that support cyber security incidence response training found in the academic literature, industrial and Government magazines, as presented in Table 1. These products show that Government and technical organizations are interested in cybersecurity and how professionals can be trained to mitigate threats for business continuity (Angafor et al., 2020; CISA, 2021; Bahuguna et al., 2019).

3. Methodology

3.1 Research Questions

The following are questions that this systematic review addressed:

RQ1. What has been the primary research focus of TTX in cybersecurity discussed in the literature?
RQ2. What are Tabletop exercises in cybersecurity published in Book Chapters, Conferences, and Journals?
RQ3. What is the distribution of book chapters, conferences, journals, and Government/Technical Organizations on TTX in cybersecurity research?

Table 1 Summary of Tabletop Exercise Products for Cybersecurity Training

TTX	Target Audience	Summary	Reference
CyberRX 2.0	CSIRTs and C-Suite executives.	TTX for the training of healthcare incident response. Multiple departments can use scenarios to determine CSIRT and team resilience readiness.	Hittrust, 2021
CISA Tabletop Exercise Packages (CTEPs)	Stakeholders in conducting their exercises	Each package includes customized exercise objectives, scenarios, discussion questions, and resources. CTEPs include scenario and module questions about pre-incident information sharing, incident response, and post-event recovery.	CTEPS, 2020
US Election Package	State, municipal, and tech election officials, media and US intelligence.	During the election season, the exercise can help keep state and local officials on their toes regarding preventing and responding to potential dangers.	Ly & Thomas, 2020
Cyber incident simulation (CIS)	Information governance, privacy, legal, compliance, internal audit, risk, and CSIRT teams.	It helps organizations practice incident response techniques, discover strengths, and address loopholes.	KPMG, 2016
Cyber wargaming	C-suite, CSIRTs, incident coordinators, and team leaders.	It helps participants educate their incident response team to handle multiple threats. It also analyses incident response personnel's threat-reaction skills.	Deloitte, 2014
Three tabletop cybersecurity TTX	CSIRT/SOC personnel	The exercise improves trainers' crisis communication skills.	Bar-Dayan, 2017
Cybersecurity incident simulation exercises (CISE)	C-suite, coordinator, and CSIRTs.	Single or many business units are trained and help C-suite executives and incident coordinators coordinate successfully.	Ernst & Young, 2017
Test your organization's incident response plan	C-Suite executives, CSIRTs, and other technical staff.	It helps C-suite managers manage crises and helps CSIRTs update incident processes.	FireEye, 2018

3.2 Literature Search Strategy

The search was undertaken between July 15th and August 15th, 2022. It centered on abstracts and citations of academic papers published in English from peer-reviewed journals, book chapters, and conferences obtained from the SCOPUS database between 2012 and 2022. The search also included Google scholar and grey literature and commercial training whitepapers, training playbooks, product description brochures, manuals, and TTX commercial evaluation reports from Cyber Defence Magazine, Info Security Magazine, and Security Magazine. Grey literature refers to materials that are outside of the traditional publications (Angafor *et al.,* 2020) Although grey literature is not formally published in the same way that traditional academic literature, such as books, journals, and conference articles. But it includes various documents, such as organizational reports and government white papers that can be highly influential in research and systematic reviews (Angafor *et al.,* 2020; Mirzaei *et al.,* 2019). In the context of this investigation, grey literature plays a

vital role since it enables research process to acquire useful data for a study. For this study, the following search criteria were utilized: "Tabletop exercise for cyber-incident response training" and "Tabletop exercises for cybersecurity, education, pedagogy, learning, teaching or training." Specifically, studies focused on game-based TTX or TTX in disaster, emergency, or disaster recovery were excluded. The Searching process was based on the Preferred Reporting Items for Systematic Reviews and meta-analyses (PRISMA) (Moher et al., 2009) The entire search strategy is shown in Fig. 1.

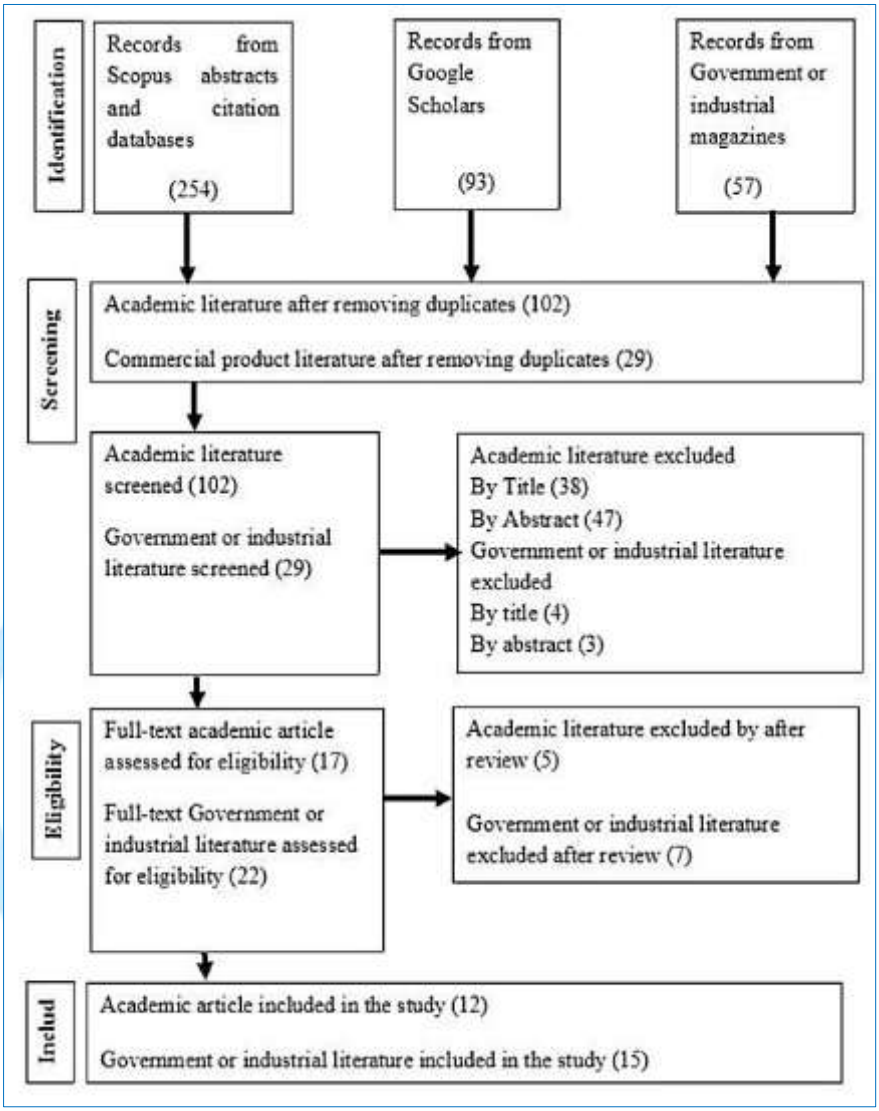

Fig. 1 A flow chart of the literature search process based on the PRISMA model

3.3 Selection and Analysis of Papers for Inclusion

There were 347 articles and abstracts returned from the academic database queries. After removing the duplicates, 102 articles remained. For inclusion in the study, the publications must discuss TTXs employed in CSIR or cybersecurity exercise training, pedagogy, education. After carefully examining all 102 articles by their abstracts, 85 were removed since they did not discuss TTXs for cybersecurity training. Thus, from the 17 articles, an additional 5 were removed because they focused on different exercise components unrelated to cybersecurity education.

The literature from organizations and Governments generated a total of 57 results. After removing the duplicates, 29 publications remained. After carefully examining all 29 publications by their abstracts, 7 were further removed using the inclusion criteria. After carefully considering the 22 publications, 7 were removed because they focused on game-based TTX, and 15 publications from Government or technical organizations were included in this study. In total, 27 pieces of literature were included in this study. The entire process is shown in Fig. 1

4. Results

The literature considered for the study is presented in Table 2, which enabled the research to address the questions stated in 3.1.

Table 2 A Summary of the main literature used in the study

Author(s)	Year	Area of focus	Source	Reference
Dewa	2018	Cyber defense using TTX	Technical research	Dewar, 2015
CIS	2018	Scenarios-based guide to TTX	Whitepaper	CIS, 2018
Everett	2016	TTX exercises for cybersecurity incident response	Whitepaper	Everett, 2016
Kick	2014	Cyber exercise playbook	Technical Report	Kick, 2015
Pacheco	2022	Analyzes of instances of tabletop simulations that led to learning of practical utility for the participants	Research Report	Pacheco, 2022
Østby *et al*.	2019	Socio-technical framework to improve cyber-security training	Conference	Østby et al. 2019
Roundtable	2021	Scenarios to help prepare for cybersecurity response	eBook	RTT, 2021
Bartels *et al*	2019	Develop innovative approaches to maximize operational effectiveness using TTX	Research Report	Bartels et al. 2019
Sitnikova *et al*	2013	TTXs for cybersecurity education.	Inform Assurance Secur. Educ. Train	Sitnikova et al., 2013
CISA/ICTAP	2022	Cybersecurity TTX and functional exercise report	Technical Report	CISA, 2022
Ulmanová		How to develop TTX for organizations	Technical Report	Ulmanová, 2021
Lynn & Raf-fety	2021	Guide to applying TTX	Technical Report	Lymn & Raffety, 2021
Hosburgh	2016	Constructing a measurable TTX in organizations	Technical Report	Hosburgh, 2016
Crimando	2017	Guide for designing TTX for organizations	Internet Resource	Crimando, 2017
Beuran *et al*	2018	Designing and implementing a framework named CyTrONE	Computer & Security	Beuran etl., 2018
Work	2021	Cybersecurity Exercises for Policy Work	Technical Report	Work, 2021
LIFEARS	2020	Cyber security training using TTX	White Paper	LIFEARS, 2020
Hobbs *et al*	2016	TTXs for education and training in the nuclear security industry.	Nuclear Security	Hobbs et al., 2016

RQ1. What has been the research focus area of TTX in cybersecurity discussed in the literature?

This question was addressed as follows; the topic of each abstract or full publication is sorted into similar objectives and focus areas, considering the knowledge areas and units in the JTF Cybersecurity Curriculum (Joint Task Force on Cybersecurity Education, 2017). The TTX for cybersecurity education is under the human security knowledge's awareness and understanding unit. Thus, the publications were grouped into the following units:

Training Guide (17): All articles that focus on guidelines and training on TTX for cybersecurity education *Framework/Model (4):* All articles focus on designing a framework/model for TTX cybersecurity education. *Measurement/Evaluation (2):* All articles focus on measuring/evaluating the impact of TTX in cybersecurity education.

Readiness/Preparedness (4): All articles focus on determining organizational readiness/preparedness using TTX for cybersecurity education.

Fig. 2 shows how often each group focus area was presented. The distributions show that the training guide is the highest, followed by framework/model and readiness and preparedness with measurement/evaluation as the least.

Fig. 2 The distribution of research focus areas of TTX in cybersecurity

Fig. 3 The growth of publications of TTX in cybersecurity

RQ2. What is the growth of Tabletop exercises in cybersecurity published in Book chapters, academic Conferences, and Journals?

Fig. 3 shows a growth of academic publications on TTX in cybersecurity. Although the growth is sparing across the period under review, there is evidence showing that TTX in cybersecurity is gaining researchers' and other stakeholders' attention and that there is a need for rigorous research to meet the dynamic of cyber-threats (Sharif & Ameen, 2020; Angafor *et al.,* 2020; Moneer & Atif, 2021).

RQ3. What is the distribution of book chapters, conferences, journals, and Government/Technical Organizations on TTX in cybersecurity research?

Fig. 4 shows the distribution of literature on TTX in cybersecurity education; the result shows that a large portion of the publication comes from Government/technical organizations, followed by journals and conference papers. These results show that research on TTX for cybersecurity education needs urgent attention from academia. Angafor *et al*. (2020) supported this assertion and called for building TTX-based learning system for developing technical and non-technical skills across academia to produce graduates who can support the increasing needs of cybersecurity experts.

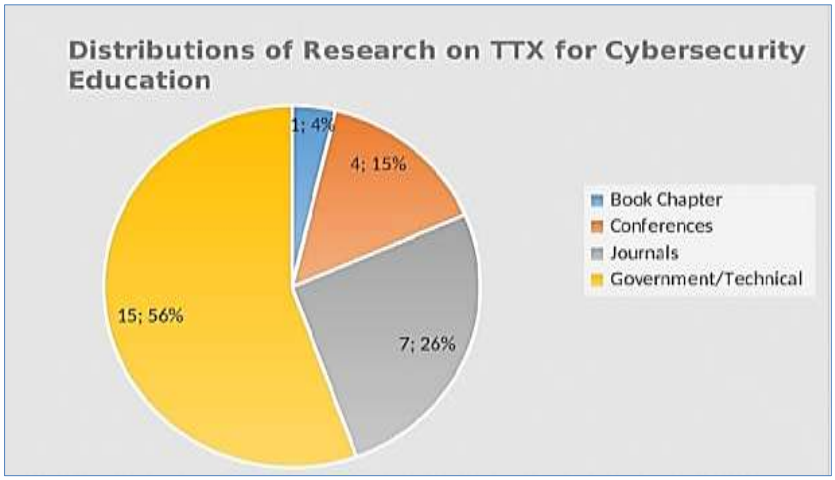

Fig. 4 The distribution of research on TTX in cybersecurity education

5. Suggestions for Further Study

Cybersecurity is a topical issue with the increasing cyber threats across organizations, and the need for cybersecurity professionals to counter and mitigate these threats is ever-increasing. TTX programs for CSIRTs need to be structured in such a way that they teach and display both technical and non-technical skills. The findings in the literature show that the security industry, governments, and regulatory agencies all show a major skills gap in the field of cyber security.

Gafic et al. (2022) and Angafor et al. (2020) noted that it is difficult for firms to hire CSIRT staff with certain skills, such as the ability to communicate, solve problems, be self-motivated, make decisions, and manage their time effectively. Thus, there is an urgent need to train graduates and CSIR experts to meet the ever-increasing cyber threat.

Thus, based on the findings of this review, several research interests can be explored by reviewing the existing literature on TTX in cyber security education. For example, findings from the review show that several guidelines for implementing TTX in cyber education, however, there is a lack of validated and generalized guidelines to support future design and implementation. Developing guidelines for designing and implementing TTX in cybersecurity needs further research. The guidelines can provide a lens through which results can be interpreted and generalized. Another area of interest is a pedagogy for supporting TTX in cybersecurity education. A pedagogy can support the TTX process for cybersecurity education. It can also be used to evaluate the impacts on the trainees and how the experiences can improve. Moreover, with the current development in smart technologies for data mining, it will be interesting to design and develop a smart learning environment taking advantage of these technologies to provide trainees with personalized and inclusive learning experiences to support TTX process for cybersecurity education. The need to develop technical and non-technical skills for the CSIRT team has several interesting questions that could be investigated in further research.

6. Conclusion

Cybersecurity has become an interested phenomenon of interested in ever increasing inter-connected world. Organizations and security experts are always seeking the best approach to mitigate these challenges through employees training and awareness. TTX has been found to be frequently used for cybersecurity education, however, there is a limited studies focused on TTX for cybersecurity education to provide insights into knowledge around TTX for further investigations. This paper reviewed publications from academic, Government and technical magazines on TTXs for cybersecurity education. The findings show that TTXs have been used for training purposes across various fields. It was discovered that TTXs are gaining popularity for CSIR training because they can enhance learning process and outcomes. It also shows that TTXs have the

potential to boost students' participation in the learning process as well as their level of drive to succeed. The findings also show that there is an increasing number of commercial TTX packages that can support cybersecurity education, and these packages can be used to support personalized learning process. This study recommends that organizations develop a systematic approach for training experts to acquire and demonstrate technical and non-technical cybersecurity skills. Similarly, TTX training should supplement traditional techniques such as classroom lectures by giving opportunities for practical learning and practice-based approaches to solving real-world problems.

Funding Information

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of Conflict

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Abbott, S. (2017). Improving Insider Threat Training, Awareness, and Mitigation Programs at Nuclear Facilities (No. SAND2017-5954R). Sandia National Lab (SNL-NM), Albuquerque, NM (United States).
2. Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Bridging the cyber security skills gap: Using tabletop exercises to solve the cssg crisis. *In Joint International Conference on Serious Games* (pp. 117-131). Springer, Cham.
3. Angafor, G.N, Yevseyeva I, He, Y.(2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. Security and Privacy. 3:e126. https://doi.org/10.1002/spy2.126
4. Aoyama, T., Nakano, T., Koshijima, I., Hashimoto, Y., & Watanabe, K. (2017). On the complexity of cybersecurity, exercises is proportional to preparedness. *Journal of Disaster Research,* 12(5), 1081-1090
5. Bahuguna, A., Raj, K.B., Jeetendra Pande (2019). Don't Wanna Cry: A Cyber Crisis Table Top Exercise for Assessing the Preparedness against Eminent Threats. *International Journal of Engineering and Advanced Technology* (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019
6. Bar-Dayan Y (2017). Tabletop Cybersecurity Training Exercises You Can Do Today. https://www.cyberbit.com/blog/security-training/3-cybersecurity-training-exercises/
7. Bartels, E. M., Grissom, A. R., Hanson, R., & Mouton, C. A. (2019). OCEANS 17 Tabletop Exercise. Rand National Defense Research Inst Santa Monica Ca Santa Monica United States.
8. Beuran, R., Tang, D., Pham, C., Chinen, K. I., Tan, Y., & Shinoda, Y. (2018). Integrated framework for hands-on cybersecurity training: CyTrONE. Computers & Security, *78*, 43-59.
9. CIS (2018). Tabletop Exercises Six Scenarios to Help Prepare Your Cybersecurity Team https://www.cisecurity.org/insights/white-papers/sixtabletop-exercises-prepare-cybersecurity-team
10. CISA (Cybersecurity & Infrastructure Security Agency) (2021). Cyber storm: Securing cyber cyberspaces://www.cisa.gov/cyber-storm-securingcyber-space. Accessed July 2022
11. CISA/ICTAP (2022). State of Oregon – Gremlins in the Gears Cybersecurity Tabletop Exercise and Functional Exercise After Action Report and provement Plan. Oregon Cyber TTX/FE AAR/IP CISA/ICTAP-OR-AFTACTRPT-004-R0. https://www.oregon.gov/siec/SiteAssets/Pages/LessonsLearned/Oregon
12. Crimando, S. (2017). The Ten Step Model for Designing Tabletop Exercise, © Everbridge
13. CTEPS (CISA Tabletop Exercise Packages) (2020). https://www.cisa.gov/cisa-tabletop-exercises-packages
14. Deloitte (2014). Prepare for the Unexpected: Cyber Threat War-Gaming Can Help Decrease the Business Impact of Cyber Incidents. Deloitte Development LLC
15. Denning, T. Lerner, A. Shostack, A and Kohno, T (2013). Control-alt-hack: the design and evaluation of a card game for computer security awareness and education. In Proc. of the 20th ACM SIGSAC conference on Computer & communications security (CCS'13), Berlin, Germany, pages 915–928. ACM Press.

16. Dewar, R. S (2018). Cyber Security and Cyber Defense Exercises. Center for Security Studies, *2018*, 6, https://css.ethz.ch/content/dam/ethz/specialinterest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf
17. ENISA (2021). Cyber exercises - cyber Europe programme. European Commission (2020). The eu's cybersecurity strategy for the digital decade. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0018&from=EN
18. Ernst & Young, E.Y. (2017). Cybersecurity Simulation Exercises: Is Simply Waiting for a Security Breach the Right Strategy? Ernest & Young Advisory Services.
19. Everett, M. (2016). Essextec White Paper – Tabletop Exercise for Cybersecurity: Maintaining a Healthy Incident Response. Essextec; 2016.
20. FireEye (2018). Tabletop Exercise: Test Your Organization's Cyber Incident Response Plan with Scenario Gameplay. FireEye Inc
21. Gafic, M., Tjoa, S., Kieseberg, P., Hellwig, O., & Quirchmayr, G. (2022). Cyber Exercises in Computer Science Education. In ICISSP (pp. 404-411).
22. HITTRUST, (2015). CyberRX 2.0 Level I Playbook. Participant and Facilitator Guide. HITRUST Alliance, LLC;
23. Hobbs, C., Lentini, L., and Moran, Matthew (2016). The Utility of Table-Top Exercises in Teaching Nuclear Security. *International Journal of Nuclear Security*, *2*(1), Article 8
24. Hosburgh, M. (2016). Constructing a Measurable Tabletop Exercise for a SCADA Environment. The SANS Institute
25. Joint Task Force on Cybersecurity Education (2017). Cybersecurity Curricular Guideline. Retrieved November 25, 2019.
26. Julius, A. A. (2014). Games and Simulations, Drills and Exercises: In-Basket Exercise, Table-top exercise, Monodrama, Role-Playing, and Role Reversal.
27. Kick, J. (2014). Cyber exercise playbook. MITRE CORP BEDFORD MA, 2014.
28. Kim, J, Maeng, Y., and Jang, M., (2019). Becoming invisible hands of national live-fire attack-defence cyber exercise. In Proc. of the 3rd IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'19), Stockholm, Sweden, pages 77–84. IEEE.
29. KPMG (2016). Cyber Incident Simulation – Be in a Defensible Position, Be Cyber Resilient. Reading, MA: KPMG International; 2016
30. Leitner, M., Frank, M., Langner, G., Landauer, M., Skopik, F., Smith, P., & Warum, M. (2021). Enabling exercises, education, and research with a comprehensive cyber range. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 12(4), 37-61.
31. LIFEARS (2020). Cybersecurity Exercises. https://www.lifars.com/tabletop-exercises/
32. Line, M. B., & Moe, N. B. (2015). Understanding collaborative challenges in its security preparedness exercises. In IFIP International Information Security and Privacy Conference (pp. 311-324). Springer, Cham.
33. Ly, O., & Thomas, J. (2020). US Elections Disinformation Tabletop Exercise Package. Berkman Klein Center Research Publication, (2020-7). https://cyber.harvard.edu/publication/2020/us-elections-disinformation-tabletop-exercise-package
34. Lynn, P. C. & Raffety, A. (2021). Cybersecurity Tabletop Exercise Guide. National Association of Regulatory Utility Commissioners (NARUC)
35. Mirzaei, S, Eftekhari A, Sadeghian M, Kazemi S, Nadjarzadeh A. (2019). The effect of disaster management training program on knowledge, attitude, and practice of hospital staff in natural disasters. J Disaster Emerg Res., *2*, 9-16. https://doi.org/10.18502/jder.v2i1.566.
36. Moher, D, Liberati A, Tetzlaff J, Altman D.G. (2009). The PRISMA Group. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. PLoS Med. 6(7):e1000097. https://doi.org/10.1371/journal.pmed1000097
37. Moneer, A., Sean .B. M., and Atif Ahmad (2021). Applying social marketing to evaluate current security education training and awareness programs in organizations. Computers & Security *100*(2021), 102090.

38. Moore, E., Fulton, S., & Likarish, D. (2017). Evaluating a multi-agency cyber security training program using pre-post event assessment and longitudinal analysis. In IFIP World Conference on Information Security Education (pp. 147-156). Springer, Cham.
39. O'Neill, A., Ahmad, A., & Maynard, S. (2021). Cybersecurity incident response in organizations: a meta-level framework for scenario-based training. arXiv preprint arXiv:2108.04996.
40. Østby, G., Berg, L., Kianpour, M., Katt, B., & Kowalski, S. J. (2019). A socio-technical framework to improve cyber security training: A work in progress. CEUR Workshop Proceedings.
41. Pacheco, F. (2022): Cybersecurity incident response tabletop simulations for learning in classrooms and organizations. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.20317416.v1
42. Rashid S. P. Anthonysamy, P., Pinto-Albuquerque, M, & Naqvi. S. (2019). The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game. IEEE Transactions on Software Engineering, 45(5):521–536.
43. RTT, (2021). Tabletop Exercise: Scenarios to Help Prepare for Cyber Security, Round Table Technology. https://www.roundtabletechnology.com/ resource-library/tabletop-exercises
44. Sabillon, R. (2022). The cybersecurity awareness training model (CATRAM). *Research Anthology on Advancements in Cybersecurity Education* (pp.501-520). IGI Global.
45. Sharif, K. H., & Ameen, S. Y. (2020). A review of security awareness approaches with special emphasis on gamification. *In 2020 International Conference on Advanced Science and Engineering* (ICOASE) (pp. 151-156). IEEE.
46. Sharkov, G., Todorova, C., Koykov, G., & Zahariev, G. (2021). A System-of-Systems Approach for the Creation of a Composite Cyber Range for Cyber/Hybrid Exercising. *Information & Security*, 50(2), 129-148.
47. Sitnikova, E., Foo, E., & Vaughn, R.B. (2013). The power of hands-on exercises in SCADA cybersecurity education. Inform Assurance Secur Educ Train., *2013*(406), 83-94.
48. Švábenský, V., Vykopal, J., & Čeleda, P. (2020). What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences. *In Proceedings of the 51st ACM technical symposium on computer science education* (pp. 2-8).
49. Švábenský, V., Vykopal, J., Čeleda, P., & Kraus, L. (2022). Applications of educational data mining and learning analytics on data from cybersecurity training. *Education and Information Technologies*, 1-34
50. Uenuma, M., Strukturer S.C. (eds.) (2018). Cybersecurity is Everyone's Job. National Initiative for Cybersecurity Education Working Group, (NICEWG), NIST.
51. Ulmanová, M. (2021). How to develop a cyber-security tabletop exercise. Technical report, National Cyber and Information Security Agency of the Czech Republic (NÚKIB).URL: https://www.nukib.cz/download/publikace/navody/cviceni/Manual_TTX_FINAL.pdf
52. Vykopal, V., Vizvary, M., Oslejsek, R., Celeda, P., & Tovarnak, D. (2017). Lessons learned from complex hands-on defense exercises in a cyber range. In Proc. of the 47th IEEE Frontiers in Education Conference (FIE'17), Indianapolis, Indiana, USA, pages 1–8. IEEE.
53. Work, C. P. (2021). Cybersecurity Exercises for Policy Work. Impulse.
54. Yamin, M. M., & Katt, B. (2019). Modelling attack and defense scenarios for cyber security exercises. In 5th interdisciplinary cyber-research conference (p. 7).