Games for Cybersecurity Decision-making

Atif Hussain, Kristen Kuhn and Siraj Shaikh

Original citation & hyperlink:
Hussain, Atif, Kristen Kuhn, and Siraj Ahmed Shaikh. "Games for Cybersecurity Decision-making." *HCI-GAMES: 2ND INTERNATIONAL CONFERENCE ON HCI IN GAMES*, Lecture Notes in Computer Science Vol 12211. Springer, 2020.

DOI: 10.1007/978-3-030-50164-8_30
ISBN: 978-3-030-50163-1
ISSN: 0302-9743

Publisher: Springer

The final publication is available at Springer via:
http://dx.doi.org/10.1007/978-3-030-50164-8_30

Games for Cybersecurity Decision-making

Atif Hussain[1], Kristen Kuhn[1], and Siraj Ahmed Shaikh[1,2]

[1]Systems Security Group, Institute for Future Transport and Cities (IFTC), Coventry University, Coventry CV1 5FB, United Kingdom
[2]Security, Risks Management and Conflict (SEGERICO) Research Group, Universidad Nebrija, 28015 Madrid, Spain

Abstract. Decision-makers are often confronted with cybersecurity challenges, which they may not fully comprehend but nonetheless need to critically address. Efficient preparation through cybersecurity games has become an invaluable tool to better prepare strategy and response to cyber incidents. Such games offer the potential for capacity building of decision-makers through a controlled environment, often presenting hypothetical scenarios that are designed to invoke discussion, while decision-making skills are put to the test. While games are acknowledged to be an effective method for such situations, many rely on technical capabilities to address these challenges. However, a key challenge is to understand the factors that influence cybersecurity decision-making. Further, game effectiveness for developing these skills is often not validated. This paper surveys cybersecurity games and compiles a data-set of 46 games to investigate how effective cybersecurity games are for assessing decision-making skills, and determines the state-of-the-art game. Through critical review and analysis of the data-set, a criteria to assess games for decision-making skills is presented. Furthermore, the criteria is applied to ten games, which determined Cyber 9/12 to be the state-of-the-art cybersecurity game for decision-making. The paper concludes with insights into how the assessment criteria can support the development of better decision-making skills through games.

Keywords: Cybersecurity Games, Decision-making, Capacity-building, Human-Computer Interaction

1 Introduction

1.1 Motivation

Cyber incidents often pose monumental threats, yet the scope and scale of their impact is not always immediately evident. Indeed, if an organisation experiences a cyber incident, the costs can carry over for years. According to a Ponemon Institute survey in 2019 [1], 507 organisations across 16 geographies and 17 industries, the average cost of a data breach was USD 3.92 million – with 67 per cent of costs occurring in the first year – and the average time it took to identify and contain a breach was over nine months.

To those charged with cyber-incident response – usually on behalf of government agencies [2], stakeholders, committees, or the public – nine months to manage a breach is difficult to justify. Those responsible are under extreme pressure to contain a breach as soon as it is discovered. If urgent response to an incident is overlooked, delayed, or compromised, then the incident may escalate into a crisis, which can be exacerbated by factors including media attention and unrest by those affected.

Decision-makers are often confronted with cybersecurity challenges they may not understand, but nonetheless need to address. Uncertainty is a key component of a crisis [3] and decision-makers must frame it as a consideration, rather than an obstacle, to respond. While cyber-incidents and their impact cannot be predicted, decision-makers can prepare strategy and response to plausible incidents, thus in turn building muscle memory to effectively react.

Efficient preparation through cybersecurity games has become an invaluable tool to improve readiness for cybersecurity decision-making. Such games offer the potential for capacity-building of decision-makers through a controlled environment, often presenting hypothetical scenarios that are designed to invoke discussion, while decision-making skills are put to the test.

1.2 Research Objectives

Human Computer Interaction (HCI) is a key element in the design of systems [4], and also in the design of games. Increasingly, manual games of all kinds, including cybersecurity games, are run on software and their parameters can be defined by computer-based tools. The processing power of a computer, along with its increased availability, means computer games are challenging manual games- especially when the topic of the game is cybersecurity [5]. HCI is redefining the meaning and the scope of games. Consequently, this study takes a multidisciplinary approach, centring on human and technology issues.

The human dimension is of particular interest in cybersecurity games as decision-makers have to make judgements about threats, risks and consequences of their actions. One challenge is to understand the factors that influence cybersecurity decision-making. In this context, this research is motivated by two research questions:

1. How effective are cybersecurity games for assessing decision-making skills?
2. What is the state-of-the-art for cybersecurity games for decision-making?

In order to answer these questions, this study develops a qualitative evaluation criteria to assess cybersecurity games for decision-making. In addition to providing a tool to conduct this study, the criteria informs the development of characteristics for strategic games, through which alignment to this criteria offers insights into how to quantify game effectiveness. The criteria is then applied to sample of cybersecurity games.

1.3 Research Contributions

This study adds to understanding of cybersecurity games five-fold: (1) It examines cybersecurity games in the context of decision-making, (2) it develops a criteria to measure game effectiveness, (3) it examines how certain observation methods are better matched to evaluation methods, (4) it identifies the state-of-the-art cybersecurity game and (5) it provides insights into how the assessment criteria can advance the development of better decision-making skills through games.

Much scientific literature on cybersecurity games [6–8] focuses on a single challenge - that of communicating abstract information to players who are not cyber-savvy. Cybersecurity is "*viewed as a niche technical subject requiring a computer science degree just to grapple with its impenetrable jargon*" [5]. While technical command of cybersecurity is an acknowledged issue amongst boards [9], policymakers [10], and public [11], it is inadequate measure of effectiveness of cybersecurity games as it overlooks a key factor: decision-making.

Cybersecurity games are a great tool to test and challenge both cybersecurity skills and decision-making skills. While previous work has surveyed cybersecurity games according to technical skills [7], no work has focused on decision-making. The starting point for this study is the assertion that cybersecurity games should not be assessed in isolation from decision-making. Therefore, this research provides unique insights into whether games are effective in developing cybersecurity decision-making skills.

This study critically reviews and analyses a range of cybersecurity games. Further, it develops a criteria to measure game effectiveness with regards to decision-making, which is a tool for the cybersecurity games community to improve games. It also examines how observation methods are better matched to certain evaluation methods. Lastly, the application of this tool is demonstrated to identify the existing state-of-the-art cybersecurity game.

1.4 Rest of this Paper

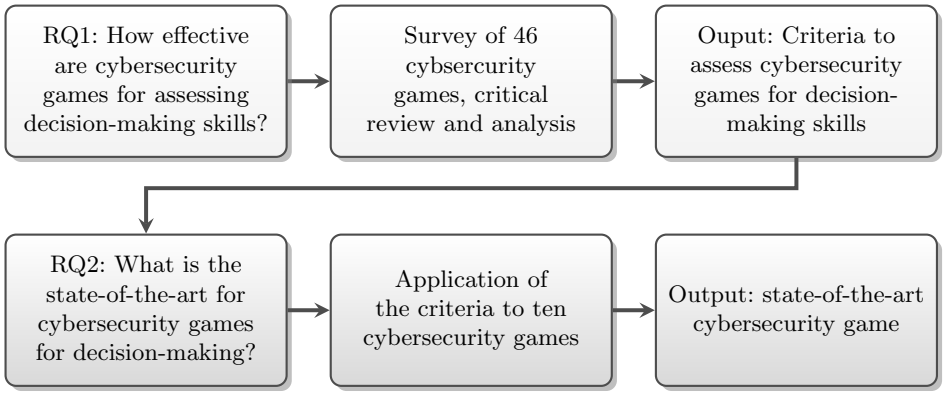
The rest of this paper is organised as follows. Section 2 presents the methodology of this study. Section 3 includes a game survey and provides a critical review and analysis of the data-set. It explains various game objectives, characteristics of scenario injects, and pairs of observation methods and evaluation methods that are effective in assessing decision-making skills. Section 4 demonstrates how the criteria can be applied to a selection of games to determine effectiveness of decision-making skills. Section 5 discusses the results and provides insights into how cybersecurity decision-makers can be better supported. Section 6 concludes this paper and outlines future work.

2 Methodology

This paper surveys cybersecurity games, and compiles a data-set by reviewing related work such as European Union Agency for Network and Information

Security (ENISA), which examined 200 cyber exercises that were executed between 2002 and 2015 [12, 13]. Desk-based research is carried out to identify additional games executed between 2016 and 2019. By grouping multiple editions of the same game, this data-set contains 67 distinct cybersecurity games. Some of the games did not provide information which was necessary for further data analysis. In order to improve the quality and reliability of results, this list is further reduced to 46 games for data analysis. Then, a qualitative approach is used to investigate this data-set by reading through available information on the games, such as game highlights, presentation and after action reports. The critical review and analysis of the data-set focuses on game objectives, scenario injects, observation methods and evaluation methods. This leads to two outcomes: (1) a criteria to assess cybersecurity games for decision-making skills which is developed through analysis of 46 games in the data-set, and (2) a conclusive finding on the state-of-the-art game, which is demonstrated by applying the criteria to a sample of ten games, which involve cybersecurity decision-making.

Fig. 1. The figure shows the research flow of this study. RQ1 is addressed through the survey of 46 games, which leads to a criteria. RQ2 is addressed through the application of this criteria to a sample of ten games, which leads to the state-of-the-art game.



3 Criteria to Assess Cybersecurity Games for Decision-making Skills

The critical review and analysis of 46 cybersecurity games is based on four main areas of typical cybersecurity game format [14–16], which includes: Game objectives, scenario injects, observation methods and evaluation methods. These provide grounds to address the research questions; and therefore, are the focus of the results presented in the subsequent section.

In response to the first research question, which asks how effective cybersecurity games are for assessing decision-making skills, a criteria is developed to score the games. The qualitative analysis of the data-set identified (1) five key themes of the game objectives, (2) characteristics of scenario injects, (3) six observation methods, and (4) four evaluation methods. The criteria is composed of these elements, and is presented in Figure 5. The 'lessons learnt' can feed into 'game design' for next edition and have the potential to improve the overall quality of the game. These two groups were not included in the criteria due to the fact that they exist outside of game-play.

3.1 Game Objectives

Game objectives were collated in a text file, which was fed into NVivo qualitative data analysis software [17] for word frequency analysis. The word grouping was matched 'with synonyms'. This matching algorithm matches words such as 'building', when it appears as build, building, established or making. The analysis returned 50 most frequent words from which five themes emerged, as shown in Table 1.

Games that include *capacity-building* are used for training or practice, and provide an environment for participants to develop skills and awareness. A focus on *decision-making* generally invokes critical thinking, and asks participants to make decisions and judgement calls. Games that have *engagement* promote cooperation and coordination internally and among other responsible organisations, often through the means of information sharing and communication outlets. Further, games with *incident management* can incite response and ask participants to manage risk factors. Finally, games that include *testing* are used to gauge preparedness by asking participants to apply procedures, processes, plans and identify areas for improvement.

Table 1. Themes emerged from game objectives analysis of 46 cybersecurity games.

Capacity-building	skills, training, awareness, practice.
Decision-making	critical
Engagement	cooperation, information sharing, communication, coordination.
Incident management	incident response, risk management.
Testing	plans, procedures, processes, identify, preparedness, improve.

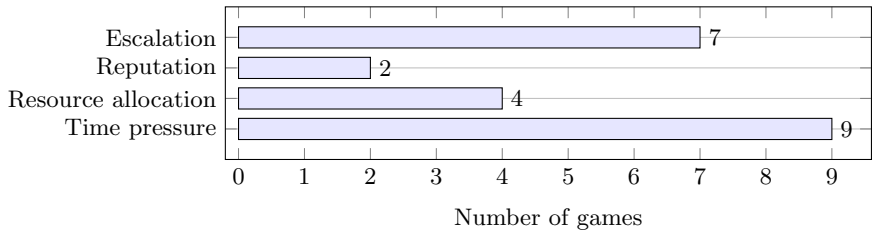
3.2 Scenario Injects

During game-play, information from a wide range of sources is provided to participants, which is a scenario inject. This can include supporting

cybersecurity evidence such as technical advisory, media items, non-confidential government or agency reports, confidential intelligence briefing, industry analysis and academic research [10]. Scenario injects can have certain characteristics such as time pressure, escalation, reputation and resource allocation, which challenges decision-making, and are shown in Figure 2.

Escalation is an increase in the severity of an incident. Cyber incidents have the potential to quickly escalate from localised incident into national emergency [18]. *Time pressure* prompts an urgent response in a timely fashion. It can be a challenge to respond effectively under pressure. *Reputation* refers to the opinions generally held about someone or something. In this context, it implies the loss or damage incurred due to a cyber incident. *Resource Allocation* refers to effective distribution of available resources.

Fig. 2. Frequency of characteristics of scenario injects in 46 cybersecurity games.

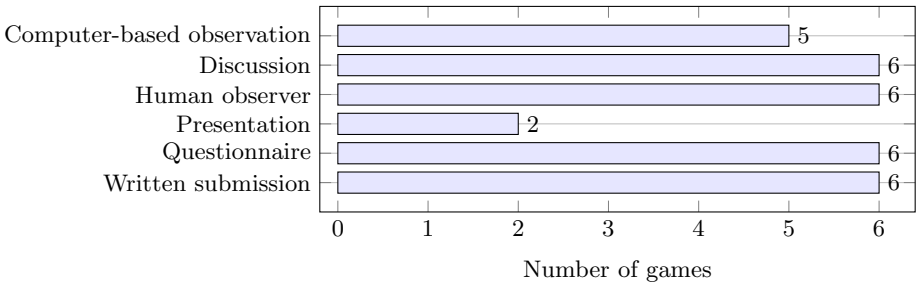


3.3 Observation Methods

Observation methods are used for data collection in the form of computer-based observation, discussion, human observer, presentation, questionnaire and written submission. These are shown in Figure 3.

Computer-based observation is the use of computers to record, calculate, and report on data collected from systematic observation, such as the use of score-bot which is a computer program that keeps track of points. *Discussion* allows participants to talk about specific topics in order to share ideas, explore various options, or reach a decision. *Human observers* are individuals or groups, who monitor game activities but do not participate in game-play. Generally, this provides game exposure to observers. Organisers may solicit feedback from observers, which can be used for game evaluation. *Presentation* involves verbally sharing experiences or results to an audience such as other participants or experts. *Questionnaire* is a survey used to gather participant feedback. *Written Submission* is a statement the participants submit to organisers in response to a scenario during game-play, such as a policy document or media engagement strategy prepared by the participants in response to a cyber incident.

Fig. 3. Frequency of observation methods in 46 cybersecurity games.

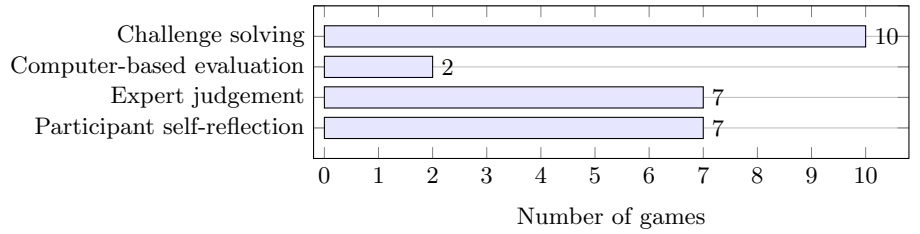


3.4 Evaluation Methods

Evaluation methods are used to gauge effectiveness of the game in the form of challenge solving, computer-based evaluation, expert judgement and participant self-reflection. These are shown in Figure 4.

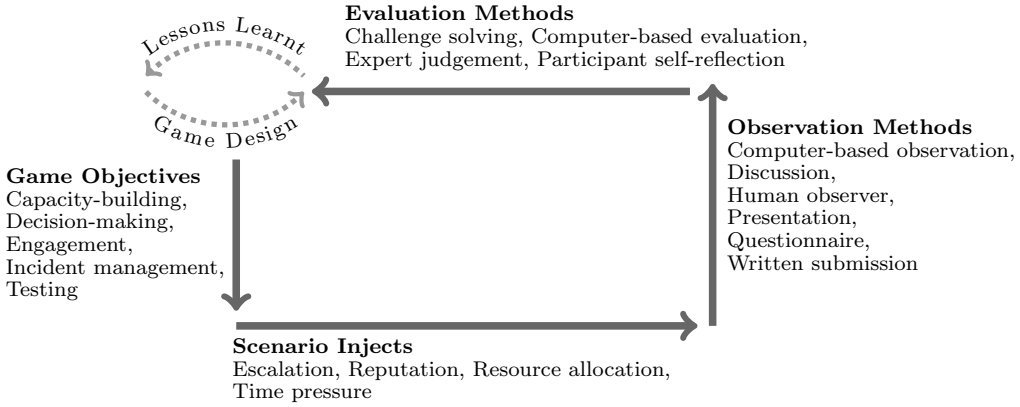
Challenge solving includes a call to participate in a competitive situation where individuals or groups compete towards an objective. For instance, a challenge can be to secure a vulnerable server, and participants have to provide a solution to secure it. *Computer-based evaluation* includes a software which keeps track of win or loose conditions, for example, in Capture The Flag (CTF) competitions the software can evaluate whether the submitted flag is correct and award points. *Expert judgement* include expert opinion or evaluation as a mode of feedback. For instance, a panel of judges may score a submission. *Participant self-reflection* includes a self-assessment. For example, an after-game survey may ask their perception of how confident they feel their skills improved from participation in the game.

Fig. 4. Frequency of evaluation methods in 46 cybersecurity games.



From the above analysis of the 46 cybersecurity games, a criteria to assess decision-making skills in cybersecurity games is established, which is shown in Figure 5. The next section applies this criteria to ten games to determine the state-of-the-art.

Fig. 5. The criteria to assess cybersecurity games for decision-making skills.



4 State-of-the-art Cybersecurity Game

In response to the second research question, which asks what is the state-of-the-art for cybersecurity games for decision-making, the criteria is applied to ten games listed in Table 2. These games were selected as they represent the diversity of games in the data-set with regards to game objectives, scenario injects, observation and evaluation methods. Game highlights, presentation and after action reports of ten cybersecurity games are examined to confirm the presence of each characteristic of the game criteria, as identified in Figure 5. For instance, if a game includes capacity-building, then it is noted (✓) in Table 3.

The criteria examines how certain observation methods are better matched to evaluation methods. Observation methods are used for data collection and feed into evaluation methods. This paper argues that specific observation methods are better matched with particular evaluation methods, e.g. computer-based observation and computer-based evaluation. This allows an effective evaluation of the cybersecurity game. Therefore, combinations of effective observation and evaluation methods are presented together in Table 3.

Table 2. A brief description of ten cybersecurity games that are selected from data-set to demonstrate the application of the criteria.

Baltic Cyber Shield: Strengthens comprehension of global cyber environment and enhances international cooperation for technical handling of incidents [19].
Blue Cascades II: Tests plans and procedures to raise awareness of infrastructure inter-dependencies, related vulnerabilities and gaps in preparedness, identifying impacts and potential solutions [20].
Cyber 9/12 Strategy Challenge: Strengthens comprehension of policy challenges relatde to cyber crisis; asks teams to respond to a hypothetical, evolving cyber-incident and analyse the national, global, and private sector threats posed [21].
Cyber Atlantic: Explores EU and US engagement and cooperation amidst cyber-attacks on their critical information infrastructures through simulated scenarios [22].
Cyberstorm: Exercises inter-agency coordination and strategic decision making to respond to an incident in accordance with state procedures and policy. [23].
GridEx: Invites industry executives and government officials to share the actions they would take and issues they would face in response to a scenario [24].
MIT Cybersecurity Simulation Game: Tests the success of decision-makers in building cybersecurity capabilities despite potential delays in capability development and in predicting cyber incidents with respect to uncertainty [25].
OZON Crisis Exercise: Tests procedures, internal collaboration and escalation processes of participants in response to technical attacks and moral dilemmas. Makes it possible to experience what its like to be targeted by a hacker group [26].
Quantum Dawn: Improves the ability of financial sector to coordinate and respond to a systemic cyber-attack, by prompting a response to a wide-scale cyber-attack [27].
White Noise: Tests coordinated central government response to a range of threats facing the UK. This programme is designed to ensure best possible response to various emergency scenarios [28].

Table 3. The criteria is used to score game effectiveness for decision-making skills. It is applied to ten games and a score out of 24 is calculated to determine state-of-the-art.

The criteria to assess cybersecurity games for decision-making skills.	Baltic Cyber Shield	Blue Cascades II	Cyber 9/12	Cyber Atlantic	Cyberstorm	GridEx	MIT	OZON	Quantum Dawn	White Noise
Game Objectives										
Capacity-building	✓	✓	✓			✓	✓	✓	✓	
Decision-making	✓		✓	✓	✓	✓	✓	✓	✓	
Engagement	✓	✓	✓	✓	✓	✓		✓	✓	✓
Incident management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Testing		✓		✓	✓	✓	✓	✓	✓	✓
Scenario Injects										
Escalation	✓		✓	✓		✓	✓	✓	✓	
Reputation			✓					✓		
Resource allocation		✓	✓		✓		✓			
Time pressure	✓		✓			✓				
Observation & Evaluation Methods										
Computer-based observation							✓			
Computer-based evaluation							✓			
Discussion		✓	✓	✓	✓	✓		✓		
Expert judgement		✓	✓	✓	✓					
Participant self-reflection		✓				✓				
Human observer	✓		✓	✓		✓		✓	✓	
Expert judgement	✓			✓				✓	✓	
Presentation			✓							
Expert judgement			✓							
Questionnaire	✓			✓	✓	✓		✓		✓
Participant self-reflection	✓			✓	✓	✓		✓		✓
Written Submission			✓			✓		✓		
Expert judgement			✓			✓				
Challenge solving			✓							
Score	10	8	16	11	9	14	8	13	8	5

Key finding - Table 3 score suggests that 'Cyber 9/12' is the state-of-the-art cybersecurity game for decision-making with a score of 16 points.

5 Discussion

While this study assesses decision-making skills in cybersecurity games, the analysis of game objectives have revealed decision-making as an objective. This was an interesting finding. Generally, technical and strategic decision-making are distinguished, but more often than not both are needed to develop a sufficient understanding of cybersecurity challenge to form an effective decision. Because technical and strategic decision-making happens simultaneously, there is no need to discern between them. This represent the complexities when exploring the human dimension of cybersecurity decision-making.

Much consideration was given in the design of scenario injects, with specific regard to the inclusion of evidence. Evidence plays significant role in the development of a scenario, providing facts that can inform a response. However, there is more to scenario injects in terms of its characteristics that triggers critical thinking and challenges decision-making, including time pressure, escalation, reputation and resource allocation. For evidence, this could extend to include conflicting or misleading information which is structured and unstructured. However, the scope of this paper includes only general characteristics of scenario injects.

It is also interesting to see that games include various aspects of decision making. While the objectives create an environment which frames decision-making, it is actually the scenario injects which trigger a response and critical thinking and challenge players to make decisions. However, of the ten games examined, almost all of them included game objectives centred around the themes that emerged, but incorporated less scenario injects. There should be greater focus on the use of diverse scenario injects to provide more opportunities for cybersecurity decision-making.

The games have their own metrics to evaluate performance. This includes both observation for data collection and evaluation. Some of these observations are easy to evaluate, such as a proof or flag could indicate a winning condition, whereas in open ended responses, judgement can be challenging. This study has captured commonly used methods and suggests how observation methods are better suited to a specific evaluation methods. When applying the criteria, it was interesting to note that no mismatch was found. This validates the proposed combinations in the template given in Table 2. The majority of observation methods include expert judgement as evaluation method, where judgement often includes assessment of observation carried out through discussion and written submission.

When the criteria was applied to ten games, the ‘Cyber 9/12 Strategy Challenge’ was found to be state-of-the-art for assessing decision-making skills of the participants. This is a two-day game, which presents cybersecurity scenarios in three rounds and asks teams to formulate a policy document. Each team presents their statement to experts, who critically review and question the teams about their written submission. Experts judge the presentation and written submission and score it. Successful teams qualify for the next round. At the end of final round, teams are given ten minutes to prepare their

response, replicating time pressure faced in real-world cyber incidents. Cyber 9/12 is an effective cybersecurity game for decision-making because it incorporates a wide range of the characteristics identified in the criteria. For instance, Cyber 9/12 includes all characteristics of scenario injects, in this case because the game includes diverse evidence items.

While the novelty of this study is most clearly pronounced in the development and identification of a state-of-the-art cybersecurity game, many other innovative findings have been established: From compiling a data-set and investigating cybersecurity games in the context of decision-making to not only developing a criteria to measure game effectiveness, but examining how certain observation methods are better matched to effective evaluation. In looking at the state-of-the-art, it also provides further insights into how assessment criteria can advance the development of better decision-making skills through games. This leads to the wider impact of this study, which adds value to the academic and cybersecurity game community. This study affirms games as an effective approach for strengthening cybersecurity decision-making, and helps to address acknowledged issue amongst boards, policymakers, and public.

6 Conclusion and Future Work

The human dimension is of particular interest in cybersecurity games as decision-makers have to make judgements about threats, risks and consequences of their actions. This paper surveys cybersecurity games and compiles a data-set. Through critical review and analysis of the data-set, it presents a criteria to determine how effective cybersecurity games are for assessing decision-making skills. The criteria is composed of game objectives, scenario injects, observation and evaluation methods. This criteria is applied to a sample of games that involve cybersecurity decision-making, to identify state-of-the-art game. Furthermore, the paper reflects on how game format and mechanisms can be improved for developing better decision-making skills.

Future work can include design-led research, where the criteria developed in this paper is used not only assess the effectiveness of cybersecurity games for decision-making skills, but to inform the design of new cybersecurity games. Indeed, design-led research techniques are proved to be clear strengths of HCI research, which have been shown to: *"Improve trust and security online, address issues such as fake news and online bias as well as improve accessibility of technologies and address sustainability of technologies"* [4]. Likewise, the criteria could also be refined through survey of more games. While 46 games informed this study, this could be extended to include a wider sample in which new trends may be incorporated into the criteria. For instance, the results are based on the available information only.

Further research in cybersecurity decision-making can provide significant benefit to the policymaking community. With the average cost of a cyber incident being USD 3.92 million, decision-makers cannot afford to not invest in effective cybersecurity decision-making.

References

1. 2019 Cost of a Data Breach Report. Technical report, Ponemon Institute, 2019.
2. Alex Chung, Sneha Dawda, Atif Hussain, Siraj Ahmed Shaikh, and Madeline Carr. *Cybersecurity: Policy*, pages 1–9. Springer International Publishing, Cham, 2018.
3. Eric Stern. *Designing Crisis Management Training and Exercises for Strategic Leaders*. 2014.
4. Jessica Bonham. Human-Computer Interaction Round Table. Technical report, Engineering and Physical Sciences Research Council, 2019.
5. Andreas Haggman. *Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education*. PhD thesis, University of London, London, UK, 2019.
6. Ajay Nagarajan, Jan M Allbeck, Arun Sood, and Terry L Janssen. Exploring Game Design for Cybersecurity Training. In *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, pages 256–262. IEEE, 2012.
7. J. Tioh, M. Mina, and D. W. Jacobson. Cyber Security Training a Survey of Serious Games in Cyber Security. In *2017 IEEE Frontiers in Education Conference (FIE)*, pages 1–5, 2017.
8. William Aubrey Labuschagne and Mariki Eloff. The Effectiveness of Online Gaming as Part of a Security Awareness Program. In *13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece*, page 125, 2014.
9. Ray A Rothrock, James Kaplan, and Friso Van Der Oord. The Board's Role in Managing Cybersecurity Risks. *MIT Sloan Management Review*, 59(2):12–15, 2018.
10. Atif Hussain, Siraj Shaikh, Alex Chung, Sneha Dawda, and Madeline Carr. *An Evidence Quality Assessment Model for Cybersecurity Policymaking*, volume 542, pages 23–38. Springer, Cham, 2018.
11. Hans de Bruijn and Marijn Janssen. Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1):1–7, 2017.
12. On National and International Cyber Security Exercises: Survey, Analysis and Recommendations. Technical report, European Network and Information Security Agency (ENISA), 2012.
13. The 2015 Report on National and International Cyber Security Exercises: Survey, Analysis and Recommendations. Technical report, European Union Agency for Network and Information Security (ENISA), 2015.
14. Evangelos Ouzounis, Panagiotis Trimintzios, and Panagiotis Saragiotis. National Exercise - Good Practice Guide. Technical report, European Network and Information Security Agency (ENISA), 2009.
15. Jason Kick. Cyber Exercise Playbook. Technical report, The MITRE Corporation, 2015.
16. Victor-Valeriu Patriciu and Adrian Constantin Furtuna. Guide for Designing Cyber Security Exercises. In *Proceedings of the 8th WSEAS International Conference on E-Activities and Information Security and Privacy*, E-ACTIVITIES'09/ISP'09, pages 172–177. World Scientific and Engineering Academy and Society (WSEAS), 2009.
17. NVivo Qualitative Data Analysis Software. available from `https://www.qsrinternational.com/nvivo/home`.

18. NCSC Cyber Attack Categorisation System for UK Incident Response, 2017. available from https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents.
19. Baltic Cyber Shield, 2010. available from https://ccdcoe.org/uploads/2018/10/BCS2010AAR.pdf.
20. Blue Cascades, 2018. available from https://www.regionalresilience.org/blue-cascades--interdependencies.html.
21. Cyber 9/12 Strategy Challenge, 2018. available from https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/cyber-912/.
22. Cyber Atlantic, 2011. available from http://www.bic-trust.eu/files/2011/12/slides15.pdf.
23. Cyber Storm I, II, III, IV, V, VI, 2018. available from https://www.dhs.gov/cyber-storm.
24. GridEx Reports, 2018. available from https://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx.
25. Mohammad S. Jalali, Michael Siegel, and Stuart Madnick. Decision-making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment. *The Journal of Strategic Information Systems*, 28(1):66–82, 2019.
26. OZON Crisis Exercise, 2016. available from https://www.surf.nl/en/node/566/whitepaper-cyber-crisis-exercise-ozon.
27. Deloitte. Quantum Dawn 2, 2013. available from https://www.sifma.org/wp-content/uploads/2013/07/after-actionreport2013.pdf.
28. White Noise - Post Exercise Public Report, 2009. available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62283/bis-exercise-white-noise.pdf.