Human Factors in Cybersecurity, Vol. 127, 2024, 137–145
https://doi.org/10.54941/ahfe1004773

Planning the Perfect Heist: An Adversarial Cyber Game

Oliver Buckley[1], Jake Montanarini[2], and Helen Quinlan[2]

[1]Loughborough University, Loughborough, UK
[2]Norwich University of the Arts, Norwich, UK

ABSTRACT

This paper introduces "Heist: An Adversarial Cyber Security Board Game", designed to enhance cyber security knowledge through interactive gameplay. Players engage in asymmetrical team-based play, simulating a 'cyber heist' on a sci-fi hotel. The unique setup integrates technical, social, and organisational strategies, enabling diverse cyber security approaches using a deck-building mechanic. *Heist* development emphasised CyBOK knowledge areas, resulting in core mechanics focused on deck building, promoting critical thinking and collaboration. Players deploy specialists to attack or defend, with attackers aiming to tarnish the hotel's reputation while the defender seeks to identify them through digital evidence. The game strikes a balance between strategy and learning, broadening participation in cyber security and deepening players' understanding of tactics. Playtesting sessions informed refinements, enhancing educational impact and entertainment value. *Heist* exemplifies an innovative approach to cyber security education, merging theory and practical application in an immersive board game format. It showcases the potential of educational games for complex subjects like cyber security.

Keywords: Cyber security, Gamification, Education, Human computer interaction, Usable security, Applied games

INTRODUCTION

In the rapidly expanding domain of cyber security, the dissemination of knowledge and the cultivation of awareness are vital. Traditional methods of education and training in this field, while effective to a degree, often struggle to engage diverse audiences and impart complex concepts in an accessible manner (Alnajim et al., 2023). The rapid advancement and the ubiquitous nature of cyber threats necessitate innovative approaches to cyber security education that are not only informative but also engaging and universally accessible. This paper introduces "Heist: An Adversarial Cyber Board Game", a pioneering educational tool designed to bridge this gap by leveraging the principles of applied gaming.

The Cyber Security Body of Knowledge (CyBOK) (Martin et al., 2024) provides a distillation of knowledge from world-leading experts to deliver the foundations the continuously expanding field of cyber security. The CyBOK comprehensively outlines essential knowledge areas (KAs) in the field of cyber security, offering a structured approach to the subject. The CyBOK itself serves as the guiding framework underpinning the development of *Heist*, with a particular focus on the Human Factors, Adversarial Behaviour, Security Operations and Incident Management, Network Security and Cyber Physical Systems KAs.

The technical nature and breadth of the material can be a daunting starting point for those wishing to develop an understanding of cyber security. This forms one of the core objectives in creating *Heist,* the game has meticulously crafted to translate these KAs into an accessible, approachable, and engaging format for a non-expert audience. Ultimately this promises to deliver cyber security education and understanding to a greater breadth of individuals, raising the overall awareness of the subject.

The motivation behind *Heist* stems from a need to address the growing gap in cyber security awareness and understanding among various stakeholders, including corporate teams, academic students, and the general public. The game aims to deliver increased cyber awareness, which has previously been shown to correlate to an individual's cyber knowledge (Zwilling et al., 2020). The increasing prevalence of cyber-related incidents only goes to underline that cyber security is no longer an issue for IT professionals, but it is a critical aspect of modern life that affects individuals and organisations across nearly all sectors. Hence, there is a pressing need for tools and methods that can effectively communicate the value of cyber security and its multifaceted nature to a broader demographic.

Heist represents a novel and significant contribution to the field of cyber security education. By utilising the engaging medium of board gaming, coupled with the foundational knowledge from CyBOK, this project aims to demystify cyber security, making it accessible and relatable to a diverse audience. The game not only serves as an educational tool but also as a medium to foster a broader and deeper appreciation of the importance and intricacies of cyber security in today's digital age.

RELATED WORK

The landscape of cyber security education is one that is quickly evolving and expanding, with game-based learning emerging as a critical tool to simplify complex concepts and engage diverse audiences. In this section we evaluate existing applications of applied games in cyber security education, with a focus on their methodologies and effectiveness. The insights gathered will contextualise the development of *Heist* highlighting its position within this innovative educational approach.

Games which rely on the use of a mobile device have been used to good effect in raising cyber awareness. The work presented by Alotaibi et al. (2017), uses this approach to deliver two specific games to educate users about malware and the importance of strong passwords, highlighting the potential to use games in engaging with a diverse audience. Similar to Alotaibi et al. (2017), *Heist* recognises the potential of games for cyber security education. However, while their work focuses on specific threats (e.g. malware), *Heist* adopts a broader perspective aligned with the CyBOK framework. This expansion of scope, alongside the engaging mechanics of a board game, aims to provide a more comprehensive and adaptable understanding of cyber security principles for diverse audiences.

Scholefield and Shepherd (2019) explore the use of gamification techniques for enhancing password security awareness and offered pertinent insights in the development of *Heist*. Like our own approach the work delivers an interactive, game-based learning to engage users and enhance their understanding of cyber security. A role-playing game (RPG) app is used to guide players through learning about password security and aligns with our own objective of using an adversarial board game to educate players about various cyber security aspects. Critical to both the RPG app and *Heist* is the emphasis on engagement and motivation in learning. Making cyber security education interactive and competitive, these tools potentially improve knowledge retention and application. The research also highlights the importance of user feedback in refining educational tools, a principle applicable to Heist for enhancing its effectiveness. However, while the paper focuses on a specific area of cyber security (password security), our own work encompasses a broader spectrum of cyber security education. This difference aside, both approaches validate the efficacy of gamification in cyber security education and underscore its importance for diverse demographics.

The use of more traditional table-top games has been applied in a range of contexts within cyber security. Riskio, developed by Hart et al. (2020) aims to deliver cyber security awareness among individuals with non-technical backgrounds, particularly within organisations. The game provides players with the opportunity to engage with both offensive and defensive roles, in a similar manner to *Heist*, providing a comprehensive understanding of cyber threats and the appropriate countermeasures. The approach taken is grounded in a constructivist learning theory, emphasising knowledge construction throughout the gameplay experience. This is an approach that encourages active collaboration and interactive learning, something that is shared by our own development. One of the key strengths of this approach is the focus on developing an engaging and accessible experience for a broader audience, an aim shared by *Heist* and the immersive nature of the scenario that has been developed.

The reviewed literature demonstrates the significant impact of gamification on cyber security education. Games like "Riskio" excel in simulating diverse cyber threats and defences through immersive board game experiences, promoting deeper awareness. Mobile applications effectively engage users while teaching specific cyber security concepts, making learning both enjoyable and accessible. Alotaibi et al. (2017) further emphasize the potential of mobile gaming to reach diverse audiences with targeted education on malware and passwords. Building upon these established successes, Heist takes a comprehensive approach guided by the CyBOK framework. Through the immersive strategies of a board game combined with foundational cyber security knowledge, Heist aims to offer a more engaging and adaptable educational experience, ultimately broadening cyber security understanding and awareness for a wider range of individuals.

DESIGN METHODOLOGY

The challenge of fusing game design methodologies with the serious intent of teaching cyber security lies in striking the right balance between making the game enjoyable and ensuring it imparts valuable knowledge about cyber threats, vulnerabilities, and best practices. This project explored the integration of game design methodologies in the development of serious games focused on cyber security education to create a market-ready product that balances enjoyment and learning.

Deterding et al. (2011) argue that to enhance user participation and a knowledge-retention-gameplay experience must follow research-led design methodologies to ensure coherent learning through intuitive design. The main design process behind Heist was a research-led method of translation, synthesis, and iteration, where key words, concepts, ideas, and meanings were distilled from the appropriate research on the subject and translated into game mechanics. This process is important to ensuring meaning, narrative, and education of key concepts (the key points expressed in the research to be communicated to the player) are at the centre of the experience.

When conducting research on the project, it was clear that the key concepts to communicate were the underlying principles of cyber security (as outlined by Martin et al. (2024)), the agency people must contribute to security and the consequences of cyber breaches through a multitude of levels of attack based on social, cultural, economic standing of the target. These elements were translated into game mechanics, rules, and procedures with varying degrees of abstractness to allow for ease of entry and access to the research material so that a diverse audience could readily engage in the ideas and themes without prior knowledge or expertise.

Upon identification, the pivotal concepts extracted from the reading material underwent a process of synthesis and evaluation, with the aim of initiating their transformation into game rules through alignment with pertinent pre-existing mechanics. As an illustration, the element of agency and decision-making within this context, whether as a subject of cyber-attacks or as an actor, was encapsulated through the implementation of deckbuilding and card management mechanics. These mechanics afford players a range of options and choices, thereby facilitating the development of strategic gameplay. Ultimately, this replicated the multitude of options when available to maintain a strong cyber security posture. In this context, the primary aim of the game functioned effectively as a puzzle-oriented competitive environment, fostering collaboration among specific players, designated as the Attackers, who were juxtaposed against another player taking on the role of the Defender. The intricacy of the puzzle presented to the players is contingent upon the actions and decisions of the Defender, an autonomous entity endowed with distinct resources and gameplay options, as they endeavour to safeguard against breaches and other cyber threats.

Heist aims to simulate real-world scenarios in a fictional setting to simultaneously replicate authentic cyber threats and security initiatives whilst adopting modes of exploration inherent to- and unbound by- play. The analogue nature of the board game enables players to explore cyber security concepts in a controlled setting, giving risk free exploration of decision-making processes that replicate real-world scenarios. Djaouti et al. (2011) argue that the benefit of simulating real-world scenarios in a ludic setting allows players to access a more profound understanding of complex subjects. In cyber security education, the use of virtual environments and simulated attacks provides a safe yet realistic platform for users to develop practical skills in identifying and mitigating security risks.

The hands-on nature of *Heist* spatially and emotionally locates the player in the scenario where interactive challenges enable the learning of security principles. This forces the player to make choices and face consequences to enhance critical and creative thinking through the intrinsic motivation, mostly set out in the win/lose set up of the game. Malone and Lepper (1987) propose that intrinsic motivation, arising from the enjoyment of an activity, is essential for effective learning.

Translating all the key points into gameplay mechanics is an important act of material gathering. Throughout the design process, every point was intricately linked to either an existing or a newly devised gameplay mechanic, poised for incorporation into various procedures. These procedures, constituting strings of rules, are integral to enabling players to construct strategic approaches, thereby fostering a sense of empowerment within the game. Consider this as the fusion of diverse elements in the game design process, where these components are refined, integrated, and structured to create a spectrum of gameplay procedures and experiences, marking the transition from foundational material to the realm of play. Subsequently, an extensive and methodical iterative process was implemented to maintain a delicate equilibrium between the enjoyable and educational aspects of the Heist gameplay experience.

When making any game that has the aim to educate and communicate, providing an experience that is both fun and challenging should be the main. Where the components you use to make the experience are distilled and translated concepts from the gathered research, the gameplay must be one that challenges the players to solve a puzzle or overcome an obstacle. This is vastly important for the communication of the ideas, as a balanced degree of challenge will keep players in a sense of flow when playing the game, a form of immersion and embedding of oneself in the experience.

Ultimately, this mode of designing is effective in its direct translation. Although, this method does require a confident understanding of common game play mechanics, it allows time to play with the different possibility of translations, thus employing exploration to ensure story and narrative (the core concepts within the research) are central.

It is important to understand what feelings and values are being designed into the experience that could be connected back to the research. When discussing potentially sensitive material and topics—such as the attacking and defending against potential cyber threats and the consequences of this—there is a danger of trivialising the material and experience for the player.

Although the discussed topic is very important, the setting of the game needed to be dehumanised in a way so that “playing” with this setting did not result in minimizing and trivialising the real-world experience of cyber threats on individuals and institutions. Thus, Heist is set in a fictional space environment and using the setting of a hotel was a design choice to keep the narrative close enough to a common player's experience to allow for a connection to the experience without feeling like a training exercise. In addition, adopting a rigid evaluative approach to the project, and ensuring the game is thoroughly play-tested, exposes any inappropriate design choices whilst establishing an audience.

Designing serious games for cyber security education requires a delicate balance between fun and learning. By incorporating research-led, explorative game design methodologies, we were able to create an engaging experience with Heist that empowers players with practical knowledge within a playful setting that increases engagement in the subject material. Continued research and innovation in this field will contribute to the development of more effective and enjoyable serious games for cyber security education.

DEVELOPMENT & INITIAL PLAYTESTING

Heist is currently at the proof-of-concept stage. Initial playtesting with the development team and other volunteers has been conducted throughout the development process to ensure gameplay is both engaging and aligns with educational goals. Feedback was overwhelmingly positive, with players highlighting the breadth of attack and defence options, and the cooperative nature of the game. A comprehensive validation study is planned using a broad range of participants across demographics, using a pre- and post-questionnaire.

THE RULES OF THE GAME

In the game, players interact with two types of boards: the Hotel board (see Figure 1) and individual Player boards. The Hotel board serves as the central playing area, depicting The Lucky Star Hotel, a renowned establishment in the Galilean system. It is where the core activities and strategies unfold. Each Player board, or "Server," (see Figure 2) represents the cyber infrastructure and resources of individual players, crucial for orchestrating attacks or defences.

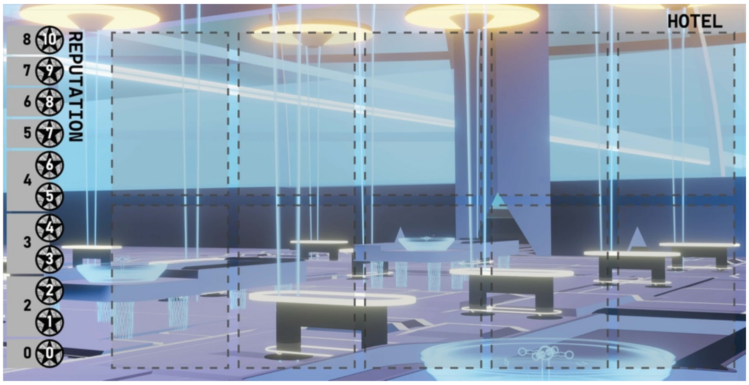

Figure 1: The Hotel board, used as a central playing area.

Heist is a deck-building game where cards are the primary tools for gameplay. There are different types of cards:

- **Heist Cards:** Used by attackers and defenders to execute various actions.
- **Specialist Cards:** Provide unique abilities to each player.
- **System Log Cards:** Central to the Defender's strategy to gather evidence against attackers.
- **Reference Cards:** Help players with game rules and strategies.
- **System Upgrade Lock Cards:** Enhance players' abilities and strategies.

Players have the option to enlist the help of *Specialists* through use of *Specialist Cards*, which provide an extra dimension to the offensive or defensive capabilities. Each player, both attackers and defenders, starts with two Specialist cards and chooses one to keep. These cards grant special abilities or actions that can be pivotal in turning the tide of the game.

The *System Log* is a dynamic element representing the hotel's recorded activities. For the Defender, it's a source to gather evidence against the attackers. The log changes as the game progresses, with each successful breach by the attackers adding new cards to it.

The attackers, a group of ethical hackers, work collectively to undermine the hotel's reputation. Their primary objective is to reduce the hotel's reputation to zero, symbolizing a complete tarnish of its public image. Each attacker utilizes a mix of Heist Cards, Specialist cards, and various resources like Data, Credits, and Time to strategize and execute their plan.

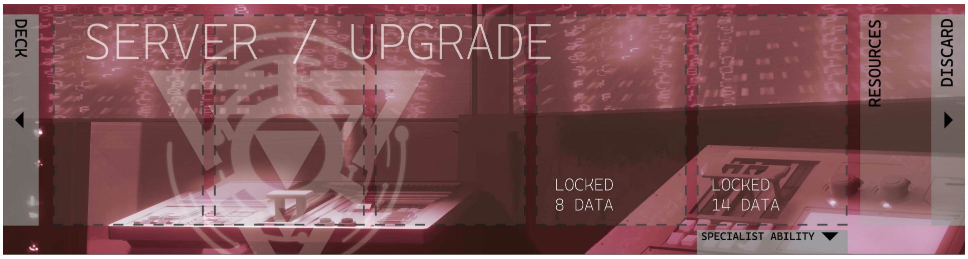

Figure 2: An example of the player (or server) board used to represent resources for individual players.

The Defender, representing the hotel owner, focuses on maintaining the hotel's reputation while uncovering the identities of the attackers. Their goal is to gather evidence from the *System Log*, which would lead to the identification of the attackers. The Defender employs *Defender Cards*, *Specialist cards*, and resources to strengthen defences and investigate breaches.

The game reaches culminates when either the attackers successfully reduce the hotel's reputation to zero, or the Defender collects five pieces of evidence from the System Log. In case of a tie, the game continues until one more successful breach or evidence is found, determining the ultimate victor.

VALIDATION AND FUTURE WORK

A formal evaluation study is planned to assess Heist's effectiveness in enhancing cyber security knowledge and awareness among a broad range of participants across various demographics. This study will employ a pre/post-test design to measure changes in knowledge levels before and after engaging with the game. Evaluation findings will be directly compared to the successes and limitations identified in the reviewed literature. This comprehensive approach aims to provide robust evidence of *Heist's* potential as an innovative and accessible cyber security education tool.

CONCLUSION

Heist represents a significant and innovative contribution to the field of cyber security education. Traditional methods of cyber security education, while valuable, often struggle to engage diverse audiences and communicate complex concepts effectively. Our work draws upon the foundational knowledge from the CyBOK and is guided by research-driven design methodologies. The game ultimately aims to bridge the gap between cyber security experts and the wider public, democratising access to critical knowledge and fostering a deeper appreciation of the subject.

The game's design process, characterized by translation, synthesis, and iteration, ensures that the core research concepts remain central to the gaming experience. Our aim in providing real-world scenarios in a fictional setting is to provide players with a safe yet immersive platform to develop practical skills in identifying and mitigating security risks. The interactivity, competitiveness, and elements of teamwork inherent in the game encourage critical thinking and enhance motivation for learning, aligning with best practices in educational game design.

The existing body of literature highlights the effectiveness of gamification in cyber security education, something that *Heist* does by offering an interactive and immersive learning experience. It builds upon the successes of other applied games and contributes to the growing recognition of gamification as a powerful tool for enhancing cyber security awareness.

Our future work will focus on further validation and exploration of the impact of *Heist*. The aim is to conduct comprehensive validation studies with both experts and non-experts in the field to assess the game's effectiveness in enhancing cyber learning and awareness, providing valuable insights into its educational impact. Additionally, *Heist* holds the potential to offer valuable insights into the practices of offensive and defensive cyber professionals. The game can serve as a platform for understanding the decision-making processes, strategies, and challenges faced by professionals in the field. This aspect of future work holds promise for elucidating the complex world of cyber operations to develop detection and analysis opportunities.

ACKNOWLEDGEMENTS

This work was supported by the Cyber Security Body of Knowledge (CyBOK) call for funded projects to develop resources around CyBOK v1.1.

REFERENCES

Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S. and Wasim, M., 2023. Exploring cybersecurity education and training techniques: a comprehensive review of traditional, virtual reality, and augmented reality approaches. Symmetry, 15(12), p. 2175.

Alotaibi, F., Furnell, S., Stengel, I. and Papadaki, M., 2017, December. Enhancing cyber security awareness with mobile games. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 129–134). IEEE.

Djaouti, D., Alvarez, J., Jessel, J. P., & Rampnoux, O. (2011). Origins of serious games. In Serious games and edutainment applications (pp. 25–43). Springer.

Hart, S., Margheri, A., Paci, F. and Sassone, V., 2020. Riskio: A serious game for cyber security awareness and education. Computers & Security, 95, p. 101827.

Malone, T. W., & Lepper, M. R. (1987). Making learning fun: A taxonomy of intrinsic motivations for learning. Aptitude, learning, and instruction, 3, 223–253.

Martin, A., Rashid, A., Chivers, H., Danezis, G., Schneider, S. and Lupu, E. (January 25, 2024) The Cyber Security Body of Knowledge (CyBOK). University of Bristol: https://cybok.org/

Scholefield, S. and Shepherd, L. A., 2019. Gamification techniques for raising cyber security awareness. In HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21 (pp. 191–203). Springer International Publishing.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H. N., 2022. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), pp. 82–97.