Security Awareness Level Evaluation of Healthcare Participants Through Educational Games

Mario Pulido[1], Christopher W. Johnson[2], Ahmed Alzahrani[3]
[1]*University of Glasgow, School of Computing Science, UK, E-mail: mpulido.infosec@gmail.com*
[2]*University of Glasgow, School of Computing Science, UK, E-mail christopher.johnson@glasgow.ac.uk*
[3] *Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia, E-mail: aaalzahrani9@kau.edu.sa*

Abstract

The purpose of this paper consists of implementing an educational board game to evaluate the information security awareness level of healthcare personnel. The National Health Service Greater Glasgow and Clyde (NHSGGC) Information Security Acceptable Use Policy was used as a basis to generate the educational content of the board game and Lev Vygotsky's social development theory was followed for the learning process of the participants. Two evaluations were carried out during this study. The results obtained during the first evaluation showed that it is fundamental to design the board game based on a set of rules in information security enacted by an organization to properly guide the participants with the knowledge they need to counter security incidents. The second evaluation showed that redesigning the content of the board game based on the information security policies of the NHSGGC, resulted in a more effective way of guiding participants on the procedures required for compliance with the policies of this health institution and offer them an understanding of the risks behind security incidents. This was demonstrated during this evaluation since the results obtained gave an approximation that it is possible to increase the level of awareness of information security in people regardless of their area of work or studies.

Keywords: *Serious games for information security; education; training; awareness; information security policies; security incidents; healthcare.*

1 Introduction

1.1 Description of the problematic reality

Today's contemporary world is surrounded by technical and industrial elements; the information age is a concept that is part of people's everyday lives. The proliferation of digital societies makes current work dependent on computer development and information technologies. The modern economy works according to the economic and numerical flows that are supported by databases [1].

Hospitals and health centres are not unaware of this reality, and health personnel are required to take into account that medical information is confidential and must remain confidential, integral, and available in the event of incidents. For this reason, information security in health centres becomes important today, and there is data that supports its value.

According to [2], "The frequency of healthcare data breaches, magnitude of exposed records, and financial losses due to breached records are increasing rapidly". This is a significant statement for this study due to the fundamental role that the health sector has in

education to comply with information security regulations, since otherwise there will be serious consequences such as the disclosure of patient information and/or economic losses.

In concordance with [3], "Cybercriminals have higher incentives to target databases with medical content in order to sell or exploit the sensitive information for their own personal gain". Cybercrime is increasingly targeting the healthcare industry, as medical information is more valuable than personal financial data or credit card details [4].

Furthermore, this problem increases when security incidents are also found to originate from insiders as the study [5, p. 374] tells on the subject, "Previous research shows that the majority of information security breaches are caused by incidents originating inside, where the internal staff is identified as the most significant threat to information security." which is relevant to this study, as internal workers are crucial to ensure that information is secured.

The causes are diverse and of different nature, for which the majority of incidents related to healthcare originate internally, and for this study, it has been detected through the review of [6,7] that this is due to the lack of an educational methodology in security awareness training.

In this paper, an educational board game is proposed to evaluate the security awareness level of healthcare staff members before and after participating in it. The material that was used as a reference for the design of the contents of the board game was based on the NHSGGC's Information Security Acceptable Use Policy [8]. Following a pre- and post-assessment, the security awareness level that participants have before and after playing the game is compared, with the purpose that it has increased at the end of their participation. Educational strategies were used to provide the correct direction of teaching and learning. Lev Vygotsky's sociocultural teaching model referenced in [9] was reviewed and adopted to ensure that the participant's learning process is acquired through forms of socialisation. For the development of the educational board game, two variables were used: awareness around behavioural ethics and the design of the board game, which has a focus on learning skills and reinforcing the existing work of the healthcare staff in terms of information security since much of their work focuses on the handling of confidential information. This study arises from the concern to maintain the integrity of the custody of medical data and the training required so that employees have the necessary knowledge to deal with security incidents.

Protecting information against disclosure, theft or damage is a public concern that does not receive sufficient awareness [10]. Therefore, this study is an example of a game developed through educational techniques to help raise awareness of healthcare personnel on the actions they can take to keep information secure.

This document is organised as follows: Section Two describes the formulation of the problem. Section Three presents the theoretical background taken as the basis for this study. Section Four details the design and elaboration of the board game and the content material. Section Five focuses on the methodology to carry out the first evaluation and the results obtained. Section Six discusses the modifications made to the game content and the results of the second evaluation applied, and Section Seven presents the limitations of the study, the conclusions, and future work.

2 Problem formulation

2.1 General problem

Healthcare personnel lack an information security educational methodology that allows them to increase their level of awareness.

2.1.1 Specific questions to address the general problem through the experiment

- How is the information security awareness level of healthcare staff members, before the implementation of the educational game?

- How is the information security awareness level of healthcare staff members, after the implementation of the educational game?

2.2 Study objectives

2.2.1 Overall objective

Implement an educational board game to assess the information security awareness level of healthcare staff members and develop an evaluation framework to validate it against learning outcomes.

2.2.2 Specific objectives

- Describe the information security awareness level of healthcare staff members, before the implementation of the educational board game.
- Describe the level of information security awareness of staff members, after the implementation of the educational board game.

3 Theoretical background

According to the study [11], "some educators have theorized that instructional games are effective for providing motivating practice of newly acquired skills and information. They have argued that instructional games are motivational because they generate enthusiasm, excitement, and enjoyment, and because they require students to be actively involved in learning". A key factor to consider in making the board game interesting enough for participants to feel motivated in learning about information security and ethical behaviour is through the use of socialisation techniques as it is considered that, from various theories of knowledge and pedagogy, people learn not only from their cognition but also from sociability [9].

In concordance to [9], the acquisition of learning techniques is explained as a form of socialisation, which means that a good level of social interaction contributes to greater knowledge. This implies that the dynamics in board games together with cognitive processes, players can improve their learning skills. It also involves the use of a mediator who guides students through the use of learning instruments during the educational process (see Figure 1).

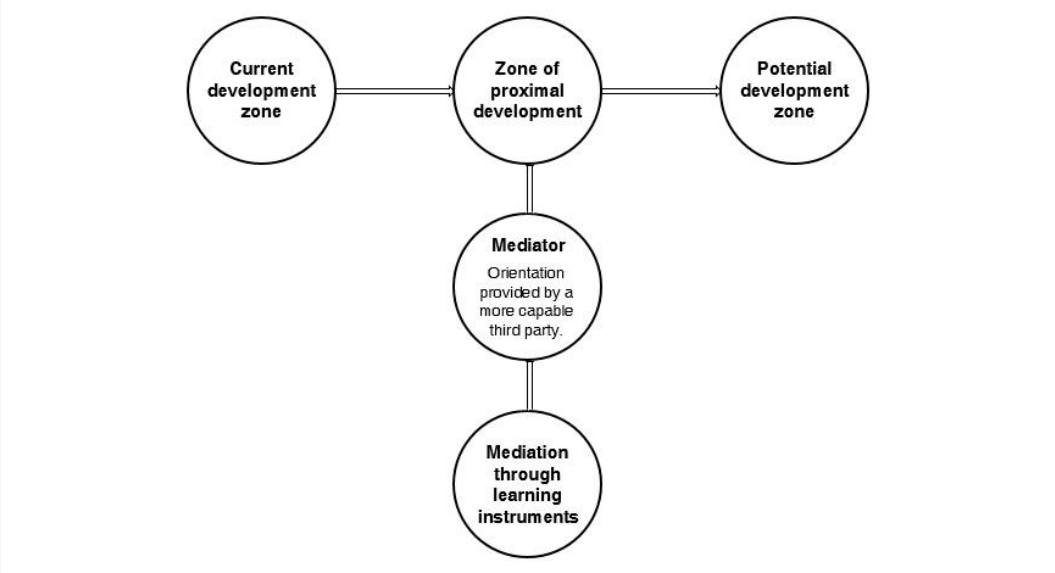


Figure 1. *Vygotsky's social development theory. Adapted from [9].*

Additionally, according to [12], games can help people consolidate their knowledge, memorise data and develop skills such as raising awareness on any subject.

The study [12], which consists of research on information security and educational games and the Control-Alt-Hack approach introduced in [13] which is an educational board game that solves missions through the use of technical skills to sensitise its target audience (people related to computer science) about compliance with information security policies in healthcare environments, were taken as a reference for the design of the board game of this study.

Games encourage socialisation and, through them, people can learn new things and reinforce the knowledge acquired. According to [14], didactic games, together with digital ecosystems, produce reactions in participants to possible incidents that may occur in real life. The study was conducted primarily to strengthen the information security awareness among participants and prevent security incidents within healthcare environments.

4 *Design of the board game*

The board game consists of an educational platform that simulates healthcare environments and whose purpose is to make participants aware of possible security incidents that put health information at risk. Players are tasked with identifying the actions that allow medical data is kept secure through critical thinking and formulating possible solutions to security incidents. Following the study [12], the game must be played by a group of three to five participants who will collaborate as a team to reduce security threats through discussion and by a game master who acts as an organiser and facilitator and provides direction and rules to follow during the game and must not intervene in the decision-making of the participants. No prior training is required.

As shown in Figure 2, the design of the board game was planned to simulate a hospital with six different rooms, which were judgmentally-selected based on the most common rooms in medical environments, also including the Management and the Information Technology (IT) departments, and each containing three security incidents. The circles represent the incidents and the rectangles located in the center of the board game consist of their description.

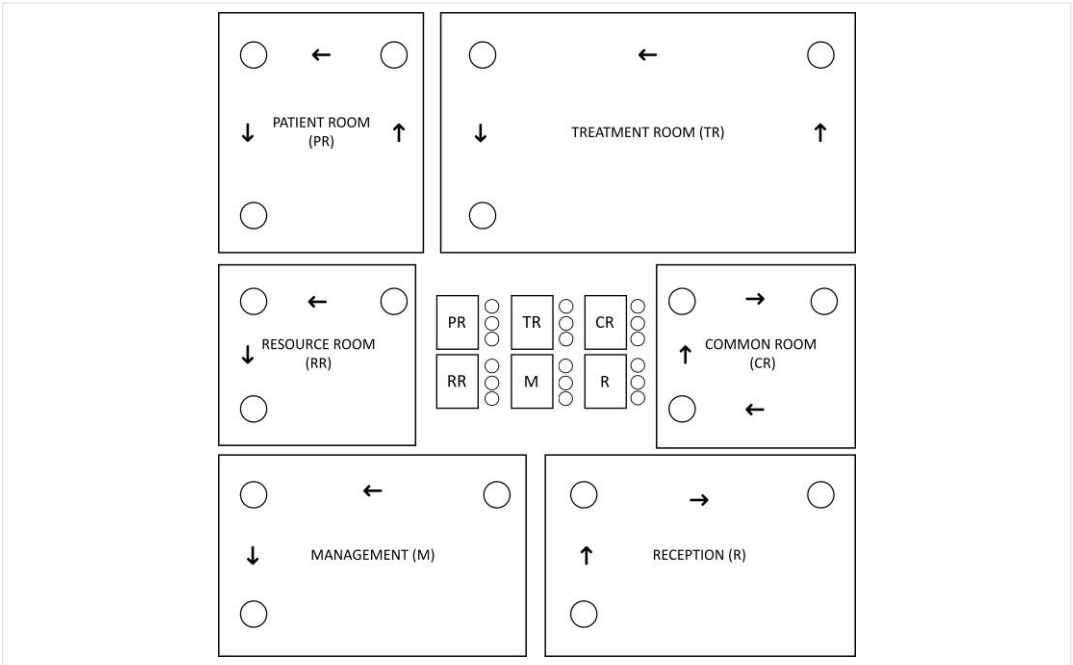


Figure 2. *Design of the board game. Photo Credit: M. Pulido.*

The categorisation of security incidents was adapted from the study [15] which consists of an introductory course for learning the fundamentals of cybersecurity and is aimed at a public without knowledge on the subject. A sample of the topics included in the study was taken, considering the security topical areas that could be of greatest interest to our participants and relevant to healthcare environments and information security. These were:

- Review the importance of using strong credentials to authenticate.
- Ethical behaviour in information security.
- Review of the ethical implications of the use of personal devices at work.
- Understand the risks of inappropriate use of social media.
- Understand the concept of a data breach, threats, and consequences.
- Review of techniques to detect phishing email.

Figure 3. *Examples of security incidents created for the board game. Photo Credit: M. Pulido.*

Upon sharing the responses to the three incidents per room, the game master provides feedback to participants to determine if their solutions are sufficient to mitigate the security incident.

4.1 Modifications to the design of the board game

4.1.1 Board game visual design

Adapted from [12], it was decided to use LEGO® as the basis for the game art and design as this would result in a more engaging, easy to understand and accessible game for players of different backgrounds and experience in information security.

4.1.2 Reduction in the number of incidents

Healthcare staff members have a strictly limited time to provide primary care to patients. The board game needed to adjust its duration to be able to satisfy the demands of the health personnel. Based on the study [16], to avoid mental distraction of participants and ensure that the game can be finished in no more than an hour the game time was intentionally kept short by reducing the number of incidents to six and allowing a maximum of ten minutes for analysis, discussions, and responses per incident. Figure 4 shows the board game design modifications leaving only one security incident per room.

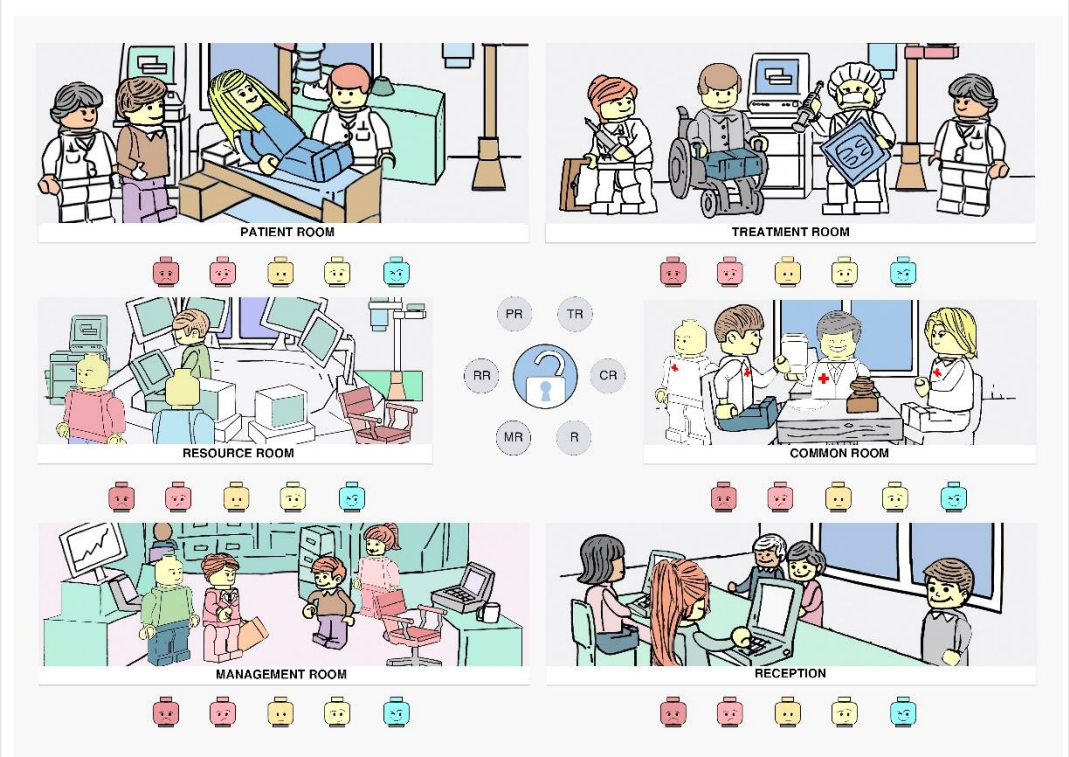


Figure 4. *Modification of the board game with six security incidents. Photo Credit: M. Pulido.*

4.1.3 Classification of participants' responses

As shown in Figure 5, a rating scale based on [17], was added to the board game which is used by the game master to rate participants' responses on a scale from very poor to very good and determine if the solution mitigates the incident based on the game master's criteria. Below is a description of these classifications:

- Very poor – Indicates unacceptable solution, greatly exceeding that the incident can be mitigated and requires an immediate response to address the incident.
- Poor – Indicates solution is unacceptable and does not meet the criteria to mitigate the incident. The hospital's room may require mitigation or response within a certain period at this level.
- Average – Indicates solution provided will have an acceptable level to mitigate the incident. At this level, no special action is required other than maintaining the solution provided.
- Good – Indicates a low level of risk. With the solution obtained, the degree of a security incident in the hospital room is reduced.
- Very good – Indicates a very low level of risk, resulting in an unlikely security incident.

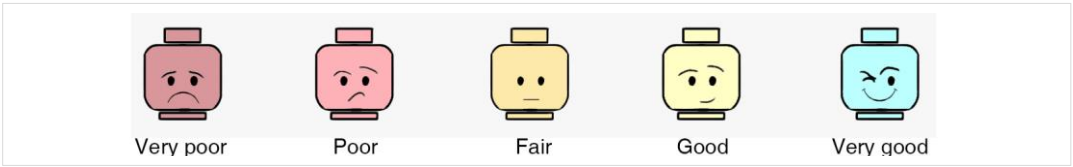


Figure 5. *Scale representation used to classify players' responses based on [17]. Photo Credit: M. Pulido.*

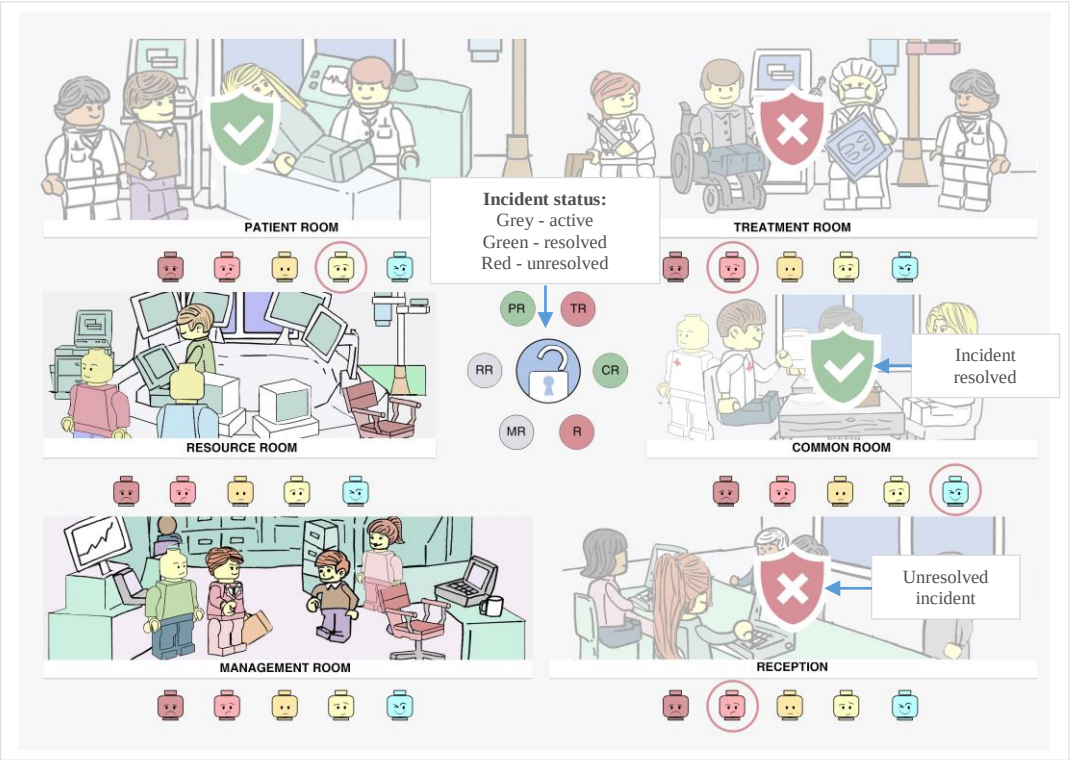


Figure 6. *Game simulation. Photo Credit: M. Pulido.*

4.1.4 Orientation guide

According to the study [18], the use of a guide in board games allows participants to better understand the terminology of the game topic. An orientation guide was designed to guide players with a brief description of information security concepts referenced in the board game. Participants use it as a reference to help them identify the best solution to security incidents. This help guide is shown in Figure 7.

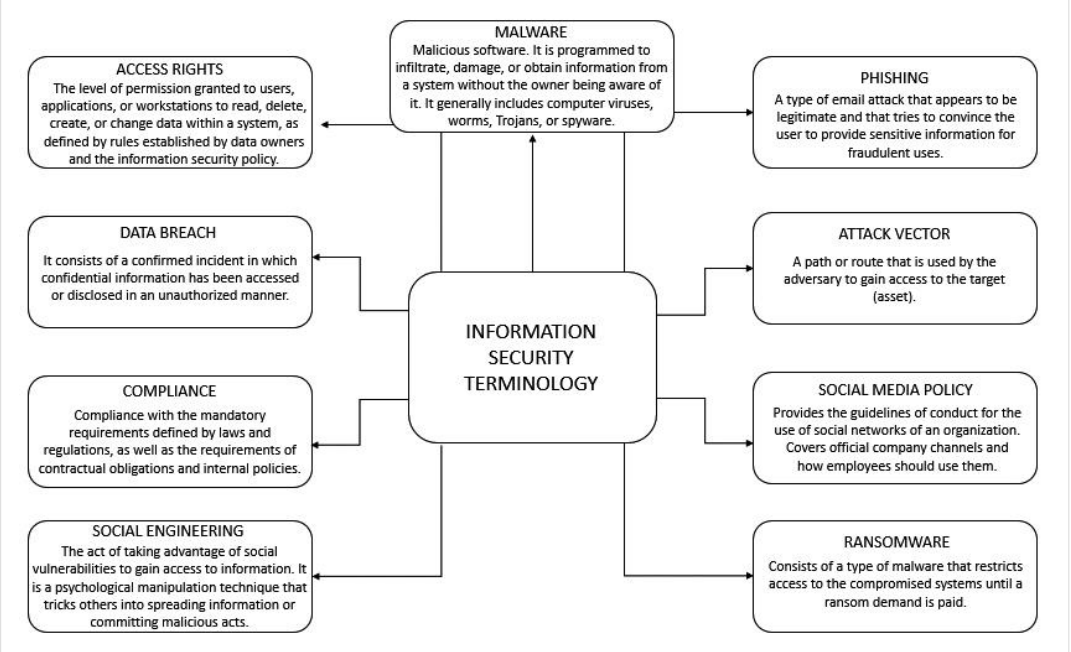


Figure 7. *Orientation guide designed for the board game. Photo Credit: M. Pulido.*

4.1.5 Pre- and post-assessments

As part of the game modification, a pre-assessment was included to be used as a basis for determining the level of security awareness before playing the game. A post-assessment followed by the completion of the game was included to determine if the learning lessons acquired had an impact on the overall security awareness levels of the participants. The pre- and post-assessments contained the same questions but in a random order to prevent participants from memorising each question.

5 First evaluation

5.1 Evaluation methodology

The type of investigation for this project consisted of an applied analysis since an experiment was carried out to evaluate the level of awareness in information security to a target audience whose studies, profession, or work are related to the healthcare field. The version of the board game detailed in Section 4.1 was used as an instrument for this evaluation and the sample obtained during the application of the experiment consisted of sixteen participants divided into four groups of three to five players.

5.1.1 Procedure for sample-collection

The pilot experiment was conducted with a group of graduate students in Sport, Exercise Science and Medicine of the University of Glasgow's School of Medicine presenting their dissertation project. A total of eleven students and five doctors were accumulated to participate in the study. They were given a participant information sheet and the purpose of the experiment and the time it would take to complete it were explained. Once they finished reading the participant information sheet, they were given a consent form to record the consent process and the participants' agreement to take part in the study. The objective of the experiment was to compare the information security awareness level of the participants before and after playing the board game and verify if it has increased after evaluating the results. The players received limited resources and their duty was to apply their judgment on incident analysis and the possible solution to the situation presented. Each of the questionnaires was given to each participant and their participation was controlled using an individual identification number.

Additionally, players also received a demographic questionnaire to track their current age, gender, occupation, and maximum level of education. The results of the demographic study applied to the participants are included in Appendix A.

Before proceeding to answer the pre-assessment questionnaire, each player was given three questions to learn about their background in information security, security awareness, and healthcare systems [12]. These questions were:

Q1. How would you rate your proficiency in information security?
Q2. How would you rate your proficiency in security awareness?
Q3. How familiar are you with healthcare systems?

At the end of the experiment, they were thanked and were told they were free to leave.

5.1.6 Findings on the first evaluation

Once the players' participation was terminated, the information of the surveys was recollected to observe the results of this evaluation and assess the level of security awareness per participant according to objectives of the study. The answers to the information security, awarenes, and healthcare systems background questionnaires are given in Table 1 below.

Table 1. *Information security background results.*

	No training or familiarity	***Some knowledge***	***Significant training or familiarity with it***	***Expert***
Q1	15	1	0	0
Q2	13	3	0	0
Q3	1	4	9	1

It was found that most of the participants did not have any formal training in information security or security awareness. Instead, the majority had significant training in healthcare systems.

The results of each participant's pre- and post-assessment surveys were summed to determine which topics players understood best and which individual topics should be reviewed. This was seen as the level of consciousness of the individual. Figure 8 shows the number of correct responses per questionnaire. Despite the interaction between the participants and the game master, it can be seen that the level of the Data Breach and Identity and Access Management controls decreased after responding to the post-assessment test, which could be due to the lack of clarity of the security incident by the players.

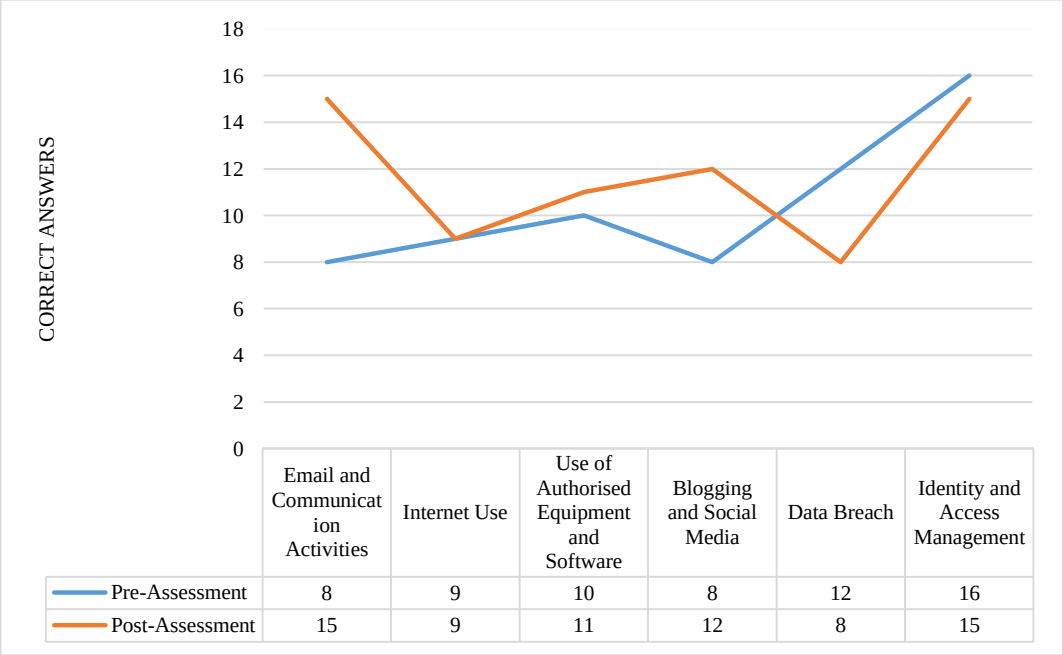
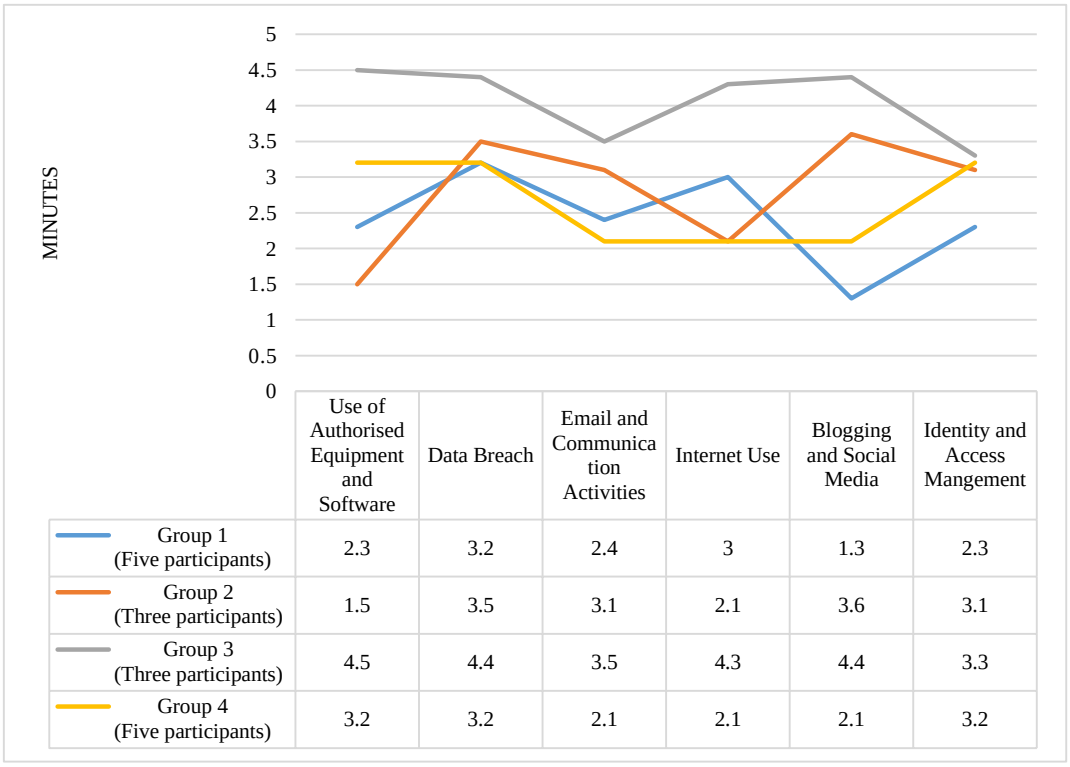


Figure 8. *Comparison of the number of correct answers in the pre- and post-assessments.*

One of the measures to be obtained through the experiment consisted in calculating the time it takes for the participants to read the incident and provide their solution to the game master. The result obtained was less than the expectation, ten minutes per incident (see Figure 9 for the time taken to provide the answer). Concerning the groups that had difficulties in formulating the response to the incidents, their time was longer compared to those groups that had a clear understanding of the presented situation who responded instinctively and their response time was less. Additionally, during the experiment, it was noted that the greater the number of participants, the shorter it took to formulate a response in contrast to the groups with fewer players, which took longer.



	Use of Authorised Equipment and Software	Data Breach	Email and Communication Activities	Internet Use	Blogging and Social Media	Identity and Access Mangement
Group 1 (Five participants)	2.3	3.2	2.4	3	1.3	2.3
Group 2 (Three participants)	1.5	3.5	3.1	2.1	3.6	3.1
Group 3 (Three participants)	4.5	4.4	3.5	4.3	4.4	3.3
Group 4 (Five participants)	3.2	3.2	2.1	2.1	2.1	3.2

Figure 9. *Time that the groups took to respond to the security incident.*

After completing the post-assessment questionnaire, the participants were asked three self-assessment questions [12] with these categories as responses: “Nothing”, “A few things”, and “A lot”.

Q1. What did you learn about information security?
Q2. What did you learn about security awareness?
Q3. What did you learn about healthcare systems?

The results corresponding to the questionnaire are shown in Table 2.

Table 2. *Knowledge level acquired results.*

	Nothing	***A few things***	***A lot***
Q1	0	8	8
Q2	0	8	8
Q3	1	9	5

Derived from the results of Table 2, it can be observed that the categories of “A few things” and “A lot” obtained the highest score, however, it is also observed that this evaluation did not achieve a significant increase in information security knowledge and awareness. It was also noted that an answer to the third question from Group 3 was missing, which can be indicated that this could have been due to an oversight by one of the participants in this group.

6 Second evaluation

The NHSGGC’s IT Compliance Team was visited and consulted to solicit feedback on the board game design and establish its validity for evaluation with healthcare staff members. They suggested modifying the content of the game based on their Information Security Acceptable Use Policy [8] and that the questionnaires and incidents should be based with

security behaviour rather than technical knowledge. Based on their observations, the pre- and post-assessment questionnaires and the security incidents were modified, taking as reference the use of [8], which provides behavioural parameters for NHSGGC staff using computer equipment and IT services.

6.1 Changes to game content

The Acceptable Use Policy [8] was studied in detail to understand and become familiar with its procedures and to adapt the content of the board game based on its security controls. It takes an approach on trust and integrity behaviours necessary to meet the security requirements of the digital age and procedures to reduce the risk of successful attack. It is organised by administrative controls that define personnel practices in accordance with NHSGGC security objectives, including the responsibilities of staff and management to ensure that their actions do not lead to computer security breaches, prevention of unauthorised access to NHSGGC systems and best practices in managing user credentials, use of authorised equipment and software to connect to the NHSGGC network, as well as correct internet usage and of emerging technologies.

A sample of six security controls was judgmentally taken for this phase of the design of the board game based on those that were considered to be most interesting to the participants. The following objectives were defined for the evaluation:

- Review the actions when receiving unwanted email and communication activities.
- Understand the correct use of the internet for personal purposes.
- Review the correct use of authorised equipment and software.
- Comprehend the responsibilities of using blogging and social media when and when not in the office.
- Understand how to properly report and keep track of security incidents and data breaches.
- Review how to keep passwords secure and confidential.

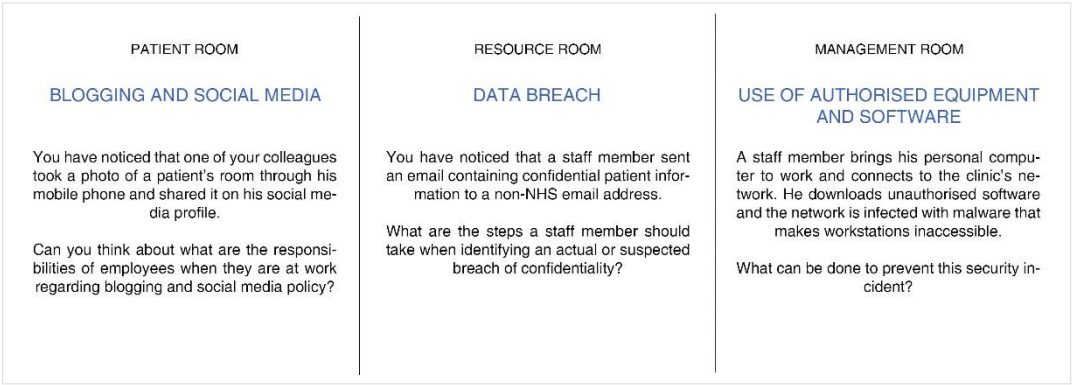


Figure 10. *Examples of security incidents modified and adapted from [8]. Photo Credit: M. Pulido.*

6.2 Changes to the orientation guide

The orientation guide that provides the information security terminology used in the previously designed board game was updated to align it with the security controls in [8] and the objectives defined in Section 6.1 in order for the participants to have a better understanding of the security incident presented and think of a solution that is better aligned with [8]. This update is shown in Figure 11.

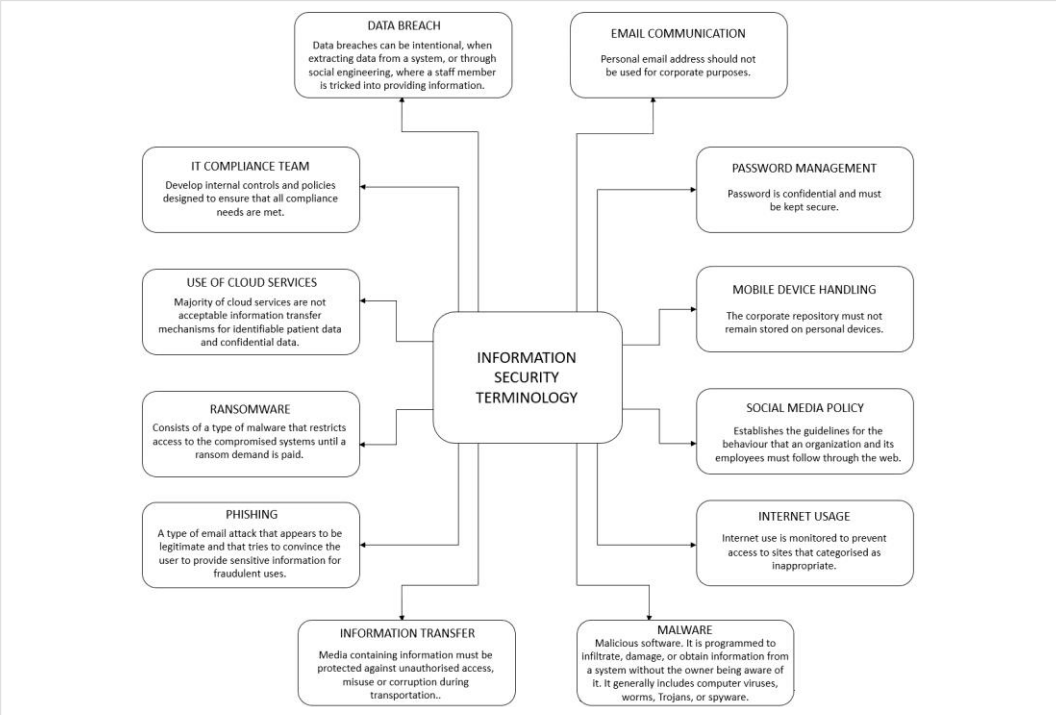
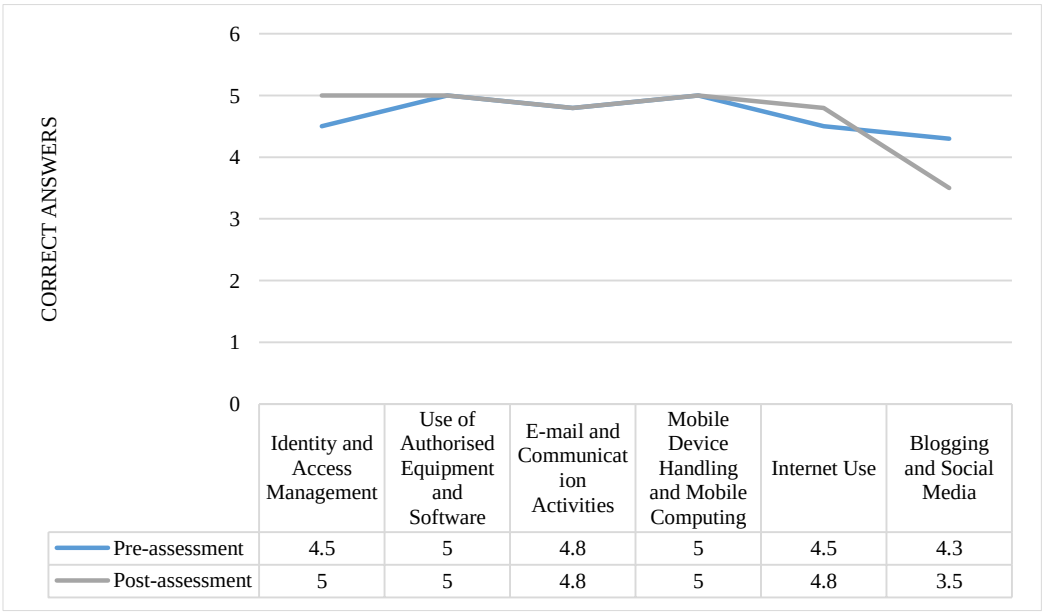


Figure 11. *Orientation guide adapted from [8]. Photo Credit: M. Pulido.*

6.3 The second evaluation applied to the NHSGGC's IT Compliance Team

Once the board game was finished modifying as per the suggestions of the NHSGGC's IT Compliance Team, they were visited a second time to apply the experiment. Four members of this team participated in the evaluation.

Figure 12 shows the results after applying the experiment to the team.



	Identity and Access Management	Use of Authorised Equipment and Software	E-mail and Communication Activities	Mobile Device Handling and Mobile Computing	Internet Use	Blogging and Social Media
Pre-assessment	4.5	5	4.8	5	4.5	4.3
Post-assessment	5	5	4.8	5	4.8	3.5

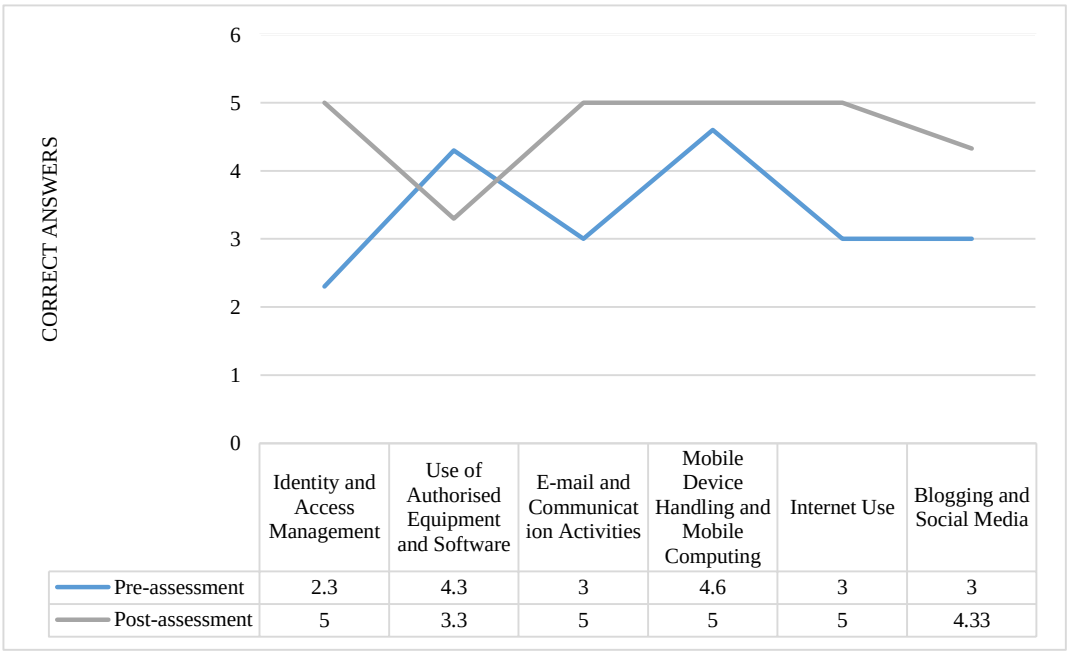
Figure 12. *The number of correct answers obtained from the test results of the NHSGGC's IT Compliance Team.*

Through the review of the results obtained from the responses of the IT Compliance Team, it was observed that the score of the post-assessment responses from the Blogging and Social Media control was lower compared to the answers of the pre-assessment and the reason behind this was because, during the game, the IT Compliance Team mentioned that although this control is included in [8] it belongs to the Human Resources department, which translates into less knowledge of this control by the IT Compliance Team.

6.4 The second evaluation applied to doctoral students

After the evaluation was carried out with the NHSGGC's IT Compliance Team, the experiment was applied this time to three Doctor of Philosophy (Ph.D.) students from the Adam Smith Business School of the University of Glasgow. Although it was necessary to apply the experiment with people from the healthcare sector, it was decided to apply the study as a pilot test to validate if a meaningful result could be obtained with the changes made through the observations from the NHSGGC's IT Compliance Team.

The responses obtained during the pre- and post-assessment were compared obtaining the results shown in Figure 13.



	Identity and Access Management	Use of Authorised Equipment and Software	E-mail and Communication Activities	Mobile Device Handling and Mobile Computing	Internet Use	Blogging and Social Media
Pre-assessment	2.3	4.3	3	4.6	3	3
Post-assessment	5	3.3	5	5	5	4.33

Figure 13. *The number of correct answers obtained from the test results of the Ph.D. students.*

When analysing the results obtained, it can be observed that the Use of Authorised Equipment and Software control decreased its score compared to the rest of the controls. This may be due to the lack of clarity in the description of the incident or through the orientation guide, but this experiment was aligned with [8], and it can be observed that it had a positive effect on the responses obtained by the participants. The time used for each incident was less than five minutes (see Figure 14), which means that it can be considered to increase the number of security incidents in the board game.

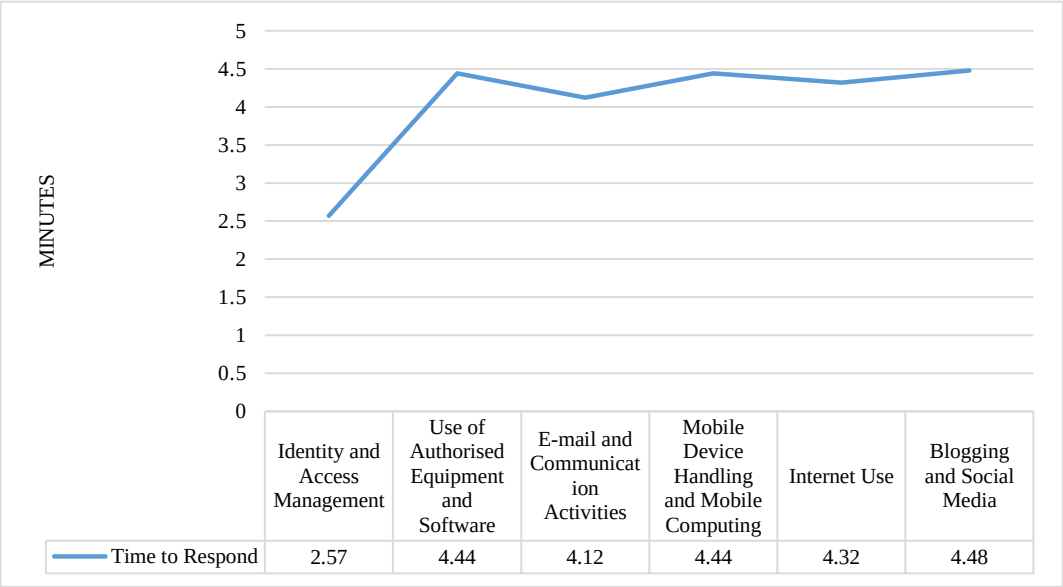


Figure 14. *Response time to security incidents of the Ph.D. students.*

7 Discussions, conclusions, and future directions

It can be observed that the sample size collected during this study was too small to have a significant result, however, it is emphasised that the applied experiment consisted of a pilot study for a larger project that is currently under development. Below is a summary of the study results:

7.1 First evaluation

During the evaluation, all the participants belonged to the healthcare field. One of them mentioned that they found it very little to have a single incident per department. The same participant mentioned he would have liked to have had a greater variety of different stories amongst the incidents including fictional characters. Feedback regarding the LEGO-based board design was positive. One participant suggested modifying the orientation guide, dividing it into sections and each one with more specific information about the security elements included in the game.

7.1.1 Limitations

It was observed that not following established information security policies as a baseline during the preparation of the material, affected the performance of the groups by not having clarity with the security incidents and the content of the board game. Additionally, two participants from one of the groups seemed to have been bored during the game and to have lost interest in participating. The complexity in understanding security terminology and a text-based game can be attributed to this behavior. Also, it was noted that the pre- and post-assessment questionnaires were not aligned with the security incidents used during the game, which made it difficult to determine if the score of the participant's level of awareness improved.

7.2 The second evaluation applied to the NHSGGC's IT Compliance Team

The [8] was used as a reference to modify the board game contents and by following the recommendations of the NHSGGC's IT Compliance Team and running the game with them

to obtain their feedback, it was possible to make improvements to the game's content in alignment with its security policies and to play a better role as the game master before applying another evaluation.

7.2.1 Limitations

Apart from the participation of the IT Compliance Team, it was not possible to get participants from the NHSGGC staff whose area is related to healthcare.

7.3 The second evaluation applied to doctoral students

The participants who were part of this evaluation better understood the information security terminology and the incident presented implying that they felt that they could apply the knowledge to real-life situations. This may be because [8] was studied in detail to align it with the content of the board game and apply it during the experiment. When analysing the responses of the participants' evaluations, it was observed that there was a good understanding of the NHSGGC' information security policies and clarity with the related incident and that this could positively impact the ethical behavior of people.

7.3.1 Limitations

The sample was small compared to the sample taken during the first evaluation and it was not possible to find participants whose field of study or work is related to healthcare, however, the players who received the second evaluation, Ph.D. Business students, did not have information security training either, therefore, it was decided to apply the experiment with them as a pilot test. After reflection, it would have been more appropriate to contact the participants who met the characteristics needed for this study with enough time in advance, as prior warning may have been more successful.

7.4 Conclusions

Education and awareness training can help mitigate security incidents that put medical information at risk. This can be accomplished by educating staff on required procedures and adherence to security policies, as well as allowing them to identify and comprehend the incident that threatens the healthcare ecosystem resulting in a secure and reliable environment. Unfortunately, there are undesirable elements that pose threats and harm to those who are not sufficiently prepared to counter attacks that threaten the security of medical data. There are several ways to keep these ecosystems protected, but, at the very least, staff members need to be educated and increase their awareness of information security incidents.

The results obtained through the first evaluation showed that participants had little clarity regarding the content of the game and this was because there was not a solid base that could be taken as a reference to generate the game and that could guide the players in developing their criteria to act ethically in the face of a security incident. Security controls can be complex, and it is essential that the awareness training is communicated in a way that staff easily understand the procedures, the security incident and its potential impact in order to apply the resulting learning into practice.

The sample used during the second evaluation involved Ph.D. business students and despite the fact that the objective of the study was to collect people related to healthcare areas and that the sample for this experiment was too small, the results obtained after applying the experiment based on [8], gave an approximation that it is possible to increase the level of information security knowledge and awareness in people regardless of whether they work in healthcare or business areas.

Additionally, following the learning theory [9], it was validated that the level of maximum potential development of the participants can be achieved through socialisation between the participants and a facilitator.

7.5 Future work

As part of the actions to be implemented in the future, it is pending to apply the modified version of the board game to people belonging to health areas and also, pending confirmation from the NHSGGC's IT Security team to conduct the study with healthcare staff members.

The use of pre- and post-assessments will continue to be used to validate if awareness level is being improved sustainably and through the information collected from the questionnaires and across the creation of performance metrics, it will be determined to reduce the existing amount of text-based content and create additional material that can help improve the effectiveness of this training.

Based on the result of the times obtained from the resolution of each incident during the evaluations, the possibility of using more than one incident for each section of the board game will be assessed. The next part of the project involves the development of the online version of the board game in order to facilitate its execution and interaction from anywhere, and to be able to carry it out in front of a greater number of healthcare participants.

8 Acknowledgments

We would like to express our deepest gratitude to the members of the NHSGGC's IT Compliance Team for allowing us to conduct this experiment with them and for their useful advice and recommendations on this project. Our thanks also go to the doctors and students of the University of Glasgow, who took part in the evaluation of this study.

References

[1] M. Cristian, "The Importance of Databases in Economy – Some General Coordinates," Revista Economica, vol. 69, issue 4, pp. 92-98, 2017.

[2] A. Seh, M. Zarour, M. Alenezi, A. Sarkar, A. Agrawal, R. Kumar, and R. Khan, "Healthcare Data Breaches: Insights and Implications," Multidisciplinary Digital Publishing Institute, vol. 2, issue 2, May 2020. https://doi.org/10.3390/healthcare8020133

[3] Pitoglou, D. Giannouli, V. Costarides, T. Androutsou, and A. Anastasiou, "Cybercrime and Private Health Data: Review, Current Developments, and Future Trends," IGI Global, 2020. https://doi.org/10.4018/978-1-5225-9715-5.ch052

[4] D. Doherty and R. Carino, "Critical risks facing the healthcare industry," Philadelphia ACE Gr., 2015.

[5] K. Hedström, E. Kolkowska, F. Karlsson, and J. P. Allen, "Value conflicts for information security management," J. Strateg. Inf. Syst., vol. 20, no. 4, pp. 373–384, 2011. https://doi.org/10.1016/j.jsis.2011.06.001

[6] J. Kamerer, D. McDermott, "Cybersecurity: Nurses on the Front Line of Prevention and Education," Journal of Nursing Regulation, vol. 10, issue 4, pp.48-53, 2020. https://doi.org/10.1016/S2155-8256(20)30014-4

[7] A. Alzahrani and C. Johnson, "Autonomy Motivators, Serious Games, and Intention toward ISP Compliance," Int. J. Serious Games, vol. 6, no. 4, pp. 67–85, 2019. https://doi.org/10.17083/ijsg.v6i4.315

[8] A.Banerjee and S.Harris., "Information Security: Acceptable Use Policy," NHS Gt. Glas. Clyde, West Cent. Scotl., vol. 1.8, 2018.

[9] J. S. Brown, C. Heath, and R. Pea, Vygotsky's educational theory in cultural context. Cambridge University Press, 2003.

[10] H. de Brujin and M. Janssen, "Building Cybersecurity Awareness: The need for evidence-based framing strategies," Science Direct, vol. 34, issue 1, pp. 1-7, January 2017. https://doi.org/10.1016/j.giq.2017.02.007

[11] J. D. Klein and E. Freitag, "Effects of Using and Instructional Game on Motivation and Performance," The Journal of Educational Research, vol. 84, no. 5, 1991. https://doi.org/10.1080/00220671.1991.10886031

[12] S. Frey, A. Rashid, P. Anthonysamy, M. Pinto-Albirquerque, and S. A. Nagvi, "The good, the bad and the ugly: a study of security decisions in cyber-physical systems game", IEEE Trans. Softw. Eng., vol. 45, no. 5, pp. 521-536, 2017. https://doi.org/10.1109/TSE.2017.2782813

[13] T. Denning, A. Lerner, A. Shostack, and T. Kohno, "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013, pp. 915–928. https://doi.org/10.1145/2508859.2516753

[14] C. C. Fung, V. Khera, A. Depickere, P. Tantatsanawong, and P. Boonbrahm, "Raising information security awareness in digital ecosystem with games-a pilot study in Thailand," in 2008 2nd IEEE International Conference on Digital Ecosystems and Technologies, 2008, pp. 375–380. https://doi.org/10.1109/DEST.2008.4635145

[15] M. Dupuis, "Cyber Security for Everyone: An Introductory Course for Non-Technical Majors," Journal of Cybersecurity Education, Research and Practice, vol. 2017, no. 1, article 3.

[16] K. Wilson and J. H. Korn, "Attention During Lectures: Beyond Ten Minutes," Teaching of Psychology, 2007. https://doi.org/10.1080/00986280701291291

[17] M. T. Di Palo, "Rating satisfaction research: is it poor, fair, good, very good, or excellent?," Arthritis Rheum. Off. J. Am. Coll. Rheumatol., vol. 10, no. 6, pp. 422–430, 1997. https://doi.org/10.1002/art.1790100610

[18] M. Thompson and C. Irvine, "Active learning with the CyberCIEGE video game," Proceedings of the 4th conference on cyber security experimentation and test, 2011. https://doi.org/10.21236/ADA547670

Appendix A (participant's profile)

Table 3. Demographic characteristics of the sample.

Variable	**Frequency**	**Percent (%)**
Gender		
Men	12	66.67
Women	4	33.33
Highest level of education		
High school	0	0
Diploma	0	0
Bachelor's	5	45.45
Master's	11	54.55
Ph.D.	0	0
Other	0	0
Age		
20-29 years	14	85.72
30-39 years	1	7.14
40-49 years	0	0
50-59 years	1	7.14