Autonomy Motivators, Serious Games, and Intention Toward ISP Compliance

Ahmed Alzahrani[1], Chris Johnson[2]
[1]*King Abdulaziz University, Faculty of Computing and Information Technology, Saudi Arabia, E-mail: aaalzahrani9@kau.edu.sa*
[2]*University of Glasgow, School of Computing Science, UK, E-mail: christopher.johnson@glasgow.ac.uk*

Abstract

The growing number of security breaches has become a major concern in organisations. Most often, such security breaches are related to internal employees due to their indirect or direct actions leading to information security policy (ISP) violations. Therefore, understanding employees' security behaviour and intrinsic motivation towards ISP compliance with respect to autonomy is critical. This study aims to find out whether the autonomy intrinsic motivator can be influenced by the Decisions and Disruptions (D-D) table-top game to enhance security awareness and, in turn, reinforce behavioural intention towards ISP compliance. We developed pre- and post-assessment tests on intrinsic motivation to find out whether there is a significant improvement in test scores after participants experience D-D gameplay. Thirty postgraduate students participated in the study. Overall results confirmed that the autonomy intrinsic motivator is positively influenced by the game and has a positive effect on the behavioural intention to comply with ISPs.

Keywords: *Serious game for cyber security; information security policy compliance; intrinsic motivation; autonomy; Self-determination theory.*

1 Introduction

The ISP of an organisation establishes a set of rules and regulations for access and use of information resources in the organisation [1] [2]. Sometimes employees do not comply with the ISP, no matter how clear the rules and regulations are. So, analysing the factors that motivate employees to adhere to the ISP has received the attention of the research community in recent years [3].

Employee behaviour is probably influenced by the behaviour of other employees the work with in groups or teams in an organisation [4]. The influencing factors involve both technical and non-technical factors dealing with protecting the sensitive information of the organisation [5]; both types of factors are equally important. Employees of an organisation can create or make possible many threats to the security of the organisation, broadly divided into two classes. The first kind of threats are intentional, involving malicious employees who leak sensitive information. The second kind of threat relates to non-intentional actions, perhaps due to carelessness, resulting in information leaks [5]. Consequently, information security is directly associated with the employee's security-related behaviour. A good understanding of employee behaviour toward compliance with an ISP can help to monitor, improve and audit staff behaviour.

Prior research considered both intrinsic and extrinsic motivation factors and employee attitudes toward complying with ISPs. Extrinsic motivation factors have been extensively studied in different mixes of rewards and sanctions. Extrinsic motivation refers to "doing something because it leads to a separable outcome" [6], such as when an employee fears sanctions for not conforming with a security policy or looks for rewards for ISP compliance. Intrinsic motivation like autonomy (See section 2) has a direct impact on compliance with policy. This suggests that intrinsic motivation to support compliance with the policy is definitely promising. Unfortunately, most of the prior research ignored intrinsic motivation factors [7] which refers to "doing something because it is inherently interesting or enjoyable" [6].

Autonomous motivation is concerned with fruitful change in behaviour over an extended period in comparison to controlled motivation by sanctions and rewards. Controlled motivation is only effective during the limited time during which its cause is active [8]. Therefore, this paper focuses on autonomy as an intrinsic motivator to enhance employees' ISP compliance through the D-D awareness cyber security game.

The literature on information security indicates that lack of information security awareness within organisations usually leads to poor ISP compliance [9][10][11]. This may expose employees to cyber-security threats, or expose their organisation to threats through them as they access the organisation's digital assets to perform routine business. However, awareness initiatives may not result in safer employee behaviour due to intentional or unintentional behavioural security incidents. This highlights the need for ways to motivate employees to behave as they know they should behave because they are self-motivated, not controlled by others. In this paper, we propose a model of intrinsic motivation validated by participation in D-D, an awareness game [12]. The model predicts that autonomy as intrinsic motivator positively influences behavioural intention towards ISP compliance, as shown in Figure 1.

Professor Rashid and his team at the University of Bristol cyber security group developed the D-D game [13]. They used the D-D game to investigate cyber security decision-making, but this paper applies the game in a different direction. Physiological theories are used to study human cyber security behaviour with respect to intrinsic motivation. We argue that by playing the game, employees can increase their security awareness, enhance their intrinsic motivation toward ISP compliance and, possibly, improve their behavioural intention to comply with ISPs outside of the game, as shown in Figure 1.

This paper is organised as follows: section 2 provides a theoretical foundation for using the autonomy intrinsic motivator in the context of information security to explain employee behaviour towards ISP compliance. Section 3 explains the game rules and instructions. Section 4 explain the link between the D-D game and the autonomy intrinsic motivator. Section 5 explains the study design, methodology and its practical elements. Section 6 presents the study analysis and results. Section 7 presents the research limitations, directions for future work and conclusions.

2 Theoretical Background

Autonomy, or the autonomous motivator, belongs to self-determination theory (SDT) which focuses on human behaviour and the extent to which behaviour is self-motivated and self- determined [14]. This theory was developed initially by researchers Edward L. Deci and Richard M. Ryan over the last 40 years. Autonomy refers to "volition, to having the experience of choice, to endorsing one's actions at the highest level of reflection"[15]. Adie *et al.* [16] argue that autonomy could support employee intrinsic motivation to comply with their organisation's rules and regulations. Wall *et al.* [17] examined the relationship between autonomy as control-related motivation and employees' behavioural intention to

comply with an ISP. The authors found a significant correlation between these two factors, which means increased perceptions of autonomy increased the perception of efficacy of intention towards ISP compliance. Also, Alzahrani *et al.* [14] developed a model to study the relationship between autonomy (among other intrinsic motivators) and behavioural intention to comply with an ISP. They found that autonomy had a positive effect on employees' behavioural intentions towards compliance with their organisation's ISP.

This paper proposes a different approach to reducing the gap between information security awareness knowledge and security-related behaviour by including autonomy as intrinsic motivator. This paper presents security awareness (to increase employees' security knowledge) in the shape of intrinsic motivation using the D-D serious game. We used security assessment tests to assess the players' awareness levels before and after the game. A heightened sense of autonomy may help employees behave as they know they should behave because they are self- determined, not controlled by others. In the end, employees may be more likely to increase their security knowledge due to the autonomy intrinsic motivator. That increased knowledge might improve their behavioural intention towards ISP compliance as shown in Figure 1.

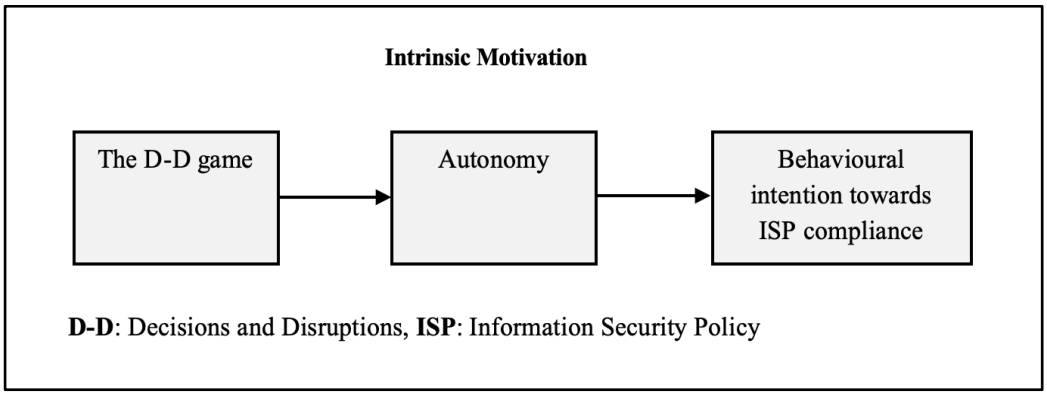

Figure 1. *A proposed research model of ISP*

3 The D-D game overview and rules

D-D is "a table-top/role-playing game about security in industrial control systems. D-D players are tasked with managing the security of a small utility company: they are given a budget that they can spend on different security options"[13]. D-D is supposed to be played by a group of two to five players under the guidance of a Game Master (GM) who controls the game.

3.1 The game board

As can be seen in Figure 2, the game board is divided into two parts: the plant where the industrialised process occurs and the office where company management and IT are located. Each part contains its local network of computers, servers and database; the two sites are connected via the internet, as shown in Figure 2. The players act as the team who are responsible for cyber security in a small company, with the objective of reducing security incidents [12]. The GM enforces the game rules during four rounds, via four steps.

- The GM explain the organisation conditions and the security infrastructure techniques.
- The GM provides the players with a budget (£100k) and explain defences (See Table 1) they can use to build the security infrastructure for the company.

- During the game, the players discuss which defences are more appropriate to prevent potential threats and determine by consensus the best way to spend their budget in each round [12].
- After each round, the GM provides the players with consequences of their investments: whether or not their defences deflected any kind of attack.

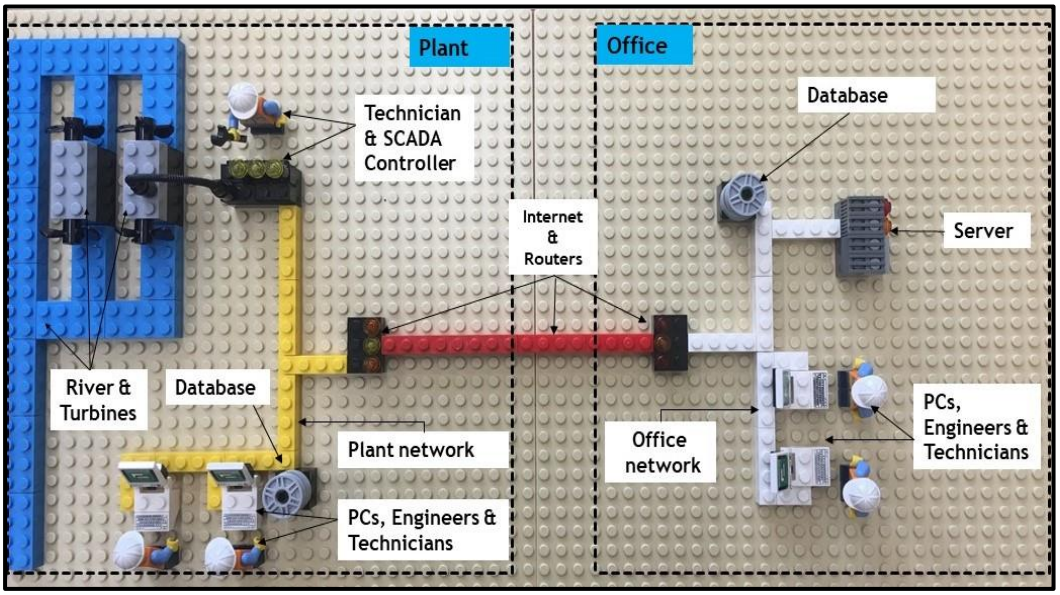

Figure 2. *Overview of the game board*

3.2 Defences

The players have a budget of (£100k) in each round, along with any unspent cash from the previous rounds. At the beginning of each round, the players need to decide which defences they should invest in to build the security infrastructure for the company, as shown in Table 1. During the game, players are given information about these defences in the form of cards.

3.3 Attacks

In each round, there are a number of attacks against the players' company infrastructure by three types of attackers. If the players invest in a Threat Assessment (See Table 1), the GM informs them about the three kinds of attackers and the attacks and objectives related to each of them.

- Script kiddies: "using basic attacks (scans, DoS, phishing, server exploits) on public targets (the company web server and email addresses)." [12].
- Organised crime: "using more advanced techniques (spear phishing, infected USB drives, infiltration via an insecure wi-fi network) to achieve more advanced goals (data exfiltration from the offices and plant, ransom based on controller disruption)." [12].
- Nation states: "using the most advanced attacks to exfiltrate technical data from the plant and disrupt the controller." [12].

Appendix A shows a specific attack that takes place during the game. Most of those attacks are silent unless the players invested in one of defences listed in Table1. For example, when the players invest in security training from Table1, the phishing attacks will be unsuccessful.

Table 1. *Initial defences available to the players. Adapted from [12].*

Defence Type	**Description**
CCTV — Plant (£ 50,000)	Surveillance cameras and alarms that will automatically warn security guards of a physical intrusion into the plant.
CCTV — Offices (£ 50,000)	Surveillance cameras and alarms that will automatically warn security guards of a physical intrusion into the offices.
Network Monitor — Plant (£ 50,000)	An advanced software and hardware solution that monitors all traffic on the plant network and detects ongoing attacks.
Network Monitor — Offices (£ 50,000)	An advanced software and hardware solution that monitors all traffic on the office network and detects ongoing attacks.
Firewall — Plant (£ 30,000)	A software and hardware solution that monitors and filters unauthorised traffic coming from the Internet to the plant network.
Firewall — Offices (£ 30,000)	A software and hardware solution that monitors and filters unauthorised traffic coming from the Internet to the office network.
Antivirus (£ 30,000)	Software protection against malware for all PCs (plant and offices).
Security Training (£ 30,000)	Basic security hygiene for all employees (plant and offices).
Asset Audit (£ 30,000)	Detailed evaluation of the company's infrastructure, reveals and shuts down any open Wi-Fi network at the plant, and unlocks additional defences.
Threat Assessment (£ 20,000)	Detailed information about possible threats and attacks against the company.
Additional Defences Available after an Asset Audit.	
Patches — Controller (£ 30,000)	Upgrade to the firmware of the SCADA controller.
Patches — PCs (£ 30,000)	Upgrade to the operating system of all PCs (plant and offices).
Patches — Server & DBs (£ 30,000)	Upgrade to the operating system of the server and databases (plant and offices).
Encryption — PCs (£ 20,000)	Encryption for all PCs (plant and offices).
Encryption — Databases (£ 20,000)	Encryption for all databases (plant and offices).

4 *The Link between the D-D Game and Autonomy Intrinsic Motivator*

This paper uses the D-D game to increase security awareness and knowledge and to strengthen autonomy intrinsic motivator. Ultimately, users are more likely to increase their security knowledge through intrinsic motivation which will, in turn, increase their behavioural intentions towards compliance. This may have a positive effect on their actual behaviour outside the game, as shown in Figure 1.

As mentioned earlier, autonomy supports the individual's desire to provide ideas and options and to have their viewpoints taken into consideration. It focuses on the desire to protect an individual's scope for action and decision-making [14]. Autonomy is supported during the game as players discuss a problem and reach a consensus for each decision they make without control or pressure from other members within the same group.

5 Study Methodology

Scenario-based assessment questions were used for this study (Appendix B). We developed the questions for both pre- and post-assessment tests to determine players' awareness knowledge levels before and after the game by measuring autonomy and behavioural intention. Each assessment test includes 14 questions, divided into two parts to cover autonomy and behavioural intention (See Section 9). There were seven scenario-based assessment questions for each part. This assessment was designed based on autonomy intrinsic motivator requirements as well as behavioural intention to comply with ISPs across four security awareness focus areas (cyber-attack, the use of email and Internet, incident response and policy compliance). For instance, to test the autonomy factor, we check the participant's security awareness level, to see if they can make a suitable decision to prevent a phishing attack. The related awareness focus areas tested within this scenario are cyber-attack, the use of email and Internet, and policy compliance-email policy. Each question may target one or more awareness focus areas. To prevent participants from memorising the questions in the pre-and post-assessment test and to minimise question order bias, we randomised the questions for use with each participant.

5.1 Refinement of Assessment Test Questions

We asked two independent researchers to conduct a final validation before distributing the questions. Their feedback was used to modify the assessment test design.

5.2 Data Collection Procedure

An invitation email was sent to the Science and Engineering Graduate School, University of Glasgow, including participant information and consent sheets to obtain responses from students. The email included a link to a site where participants could complete a form to arrange a convenient time and location to take part in the study. Since this study involves a face-to-face focus group discussion, each group of participants were in the same room to play the game together, with the experimenter or GM to control the game.
There were 30 participants divided into six groups, so each group had five players (the game rules recommend a group of two to five players). Group selection was random, based on participant availability. The participants' profiles for all six groups are summarised in section 10. Each game, together with the evaluation, lasted up to two hours. The study was approved by the relevant ethics committee.

5.3 Study Procedures

The sequence of steps followed in this study can be seen in Figure 3. The first step is to assess each participant's awareness level through a paper-based pre-assessment test. The assessment does not include participants' names or emails. We used Group IDs such as Group A and player IDs to link pre-assessment and post-assessment test scores to find out each participant's overall score before and after the game and to compare the scores. A participant could choose any player ID that nobody else had chosen. Their names, emails, and other personally identifiable information remain anonymous. At the end of the game, we gave the participants a paper-based assessment (post-assessment test) to determine their overall security awareness. After that, the players were thanked for participating and were told they were free to leave.

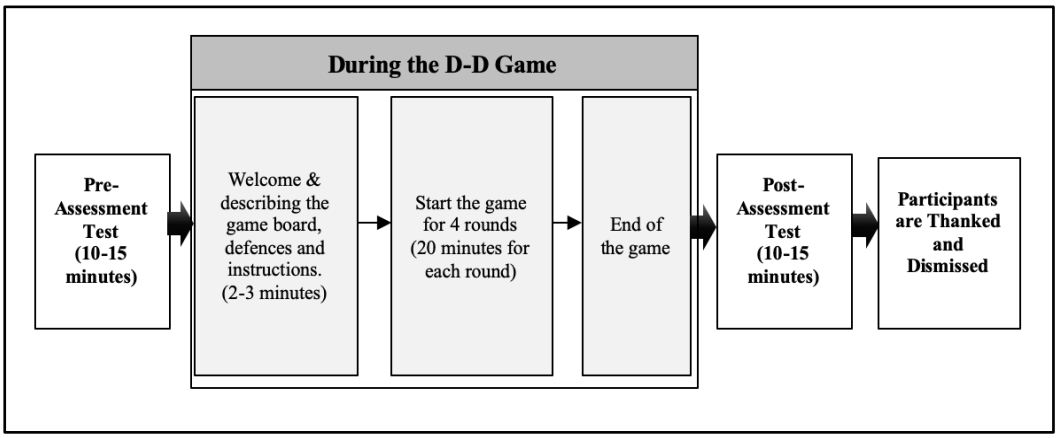

Figure 3. *Assessment and Game Flow*

6 Data Analysis and Results

6.1 Data Analysis Method

We followed three steps to analysis the collected data for each factor:

- Pre-assessment test: The pre-assessment test score was used to determine the players' autonomy and intention to comply with an ISP before the game.
- During the game: We followed the requirements of the autonomy factor as well as taking notes of our observations during the game to analyse players' behaviour. The link between the autonomy intrinsic motivator and the D-D game is explained in detail in section 4. We focused on group discussion during all four rounds in the game to learn whether each player provided his/her ideas and viewpoints without control or pressure from other group members, and joined by consensus in the group's decisions. We also wanted to find out whether the group's decisions prevented attacks for each round.
- Post-assessment test: The post-assessment test score was used to determine the players' autonomy and ISP compliance intention after the game to find out whether they benefited from the game.

6.2 The Use of Awareness Measurement for Data Analysis

Table 2 shows the scale that was used to interpret the level of awareness for assessment tests. This scale was adapted from Kruger and Kearney [18]. They used this scale to develop a prototype model for measuring employee security behaviour, attitude and knowledge. Hence, we found this scale is suitable for this study because of its focus in studying human security behaviour. For example, in Figure 4 (group A), the post-assessment test score for the autonomy factor is 90% which mean the average score for this group is at the Good level (range of scores from 80-100) as explained in Table 2. We followed the same technique to compute the overall result of pre- and post-assessment tests for all participants, as summarised in Tables 3 and 4. For example, in Table 3, the average score for the four awareness focus areas across the autonomy factor is 59% which is at the Poor level based on the measurement in Table 2. The Table 2 also presents the percentage for each awareness focus area, which makes it easy to review the level of awareness of each intrinsic factor or intention and take the required action. This scale is suitable for this study because it was designed to study employees' security behaviour. The scale could be changed by further studies without compromising the overall approach used and depending on the criticality of the environment.

Table 2. *Awareness Level Measurement*

Awareness Level	Measurement (%)	Action
Good	80-100	Satisfactory – no need for action
Average	60–79	Monitor – action potentially required
poor	59 and less	Unsatisfactory – action required

6.3 *The Use of Pre and Post- Assessment Tests Result for Intrinsic Motivation Analysis*

Figure 4 shows mean values from individual assessment tests of the autonomy factor and intention to comply with an ISP for each group before and after the game. The overall result for all groups is presented in Table 3 and 4. We used the results in the qualitative analysis (to compare the group members' security behaviour during the game with the test results) to provide an in-depth analysis of the autonomy intrinsic motivator, as discussed in detail in section 6.5.

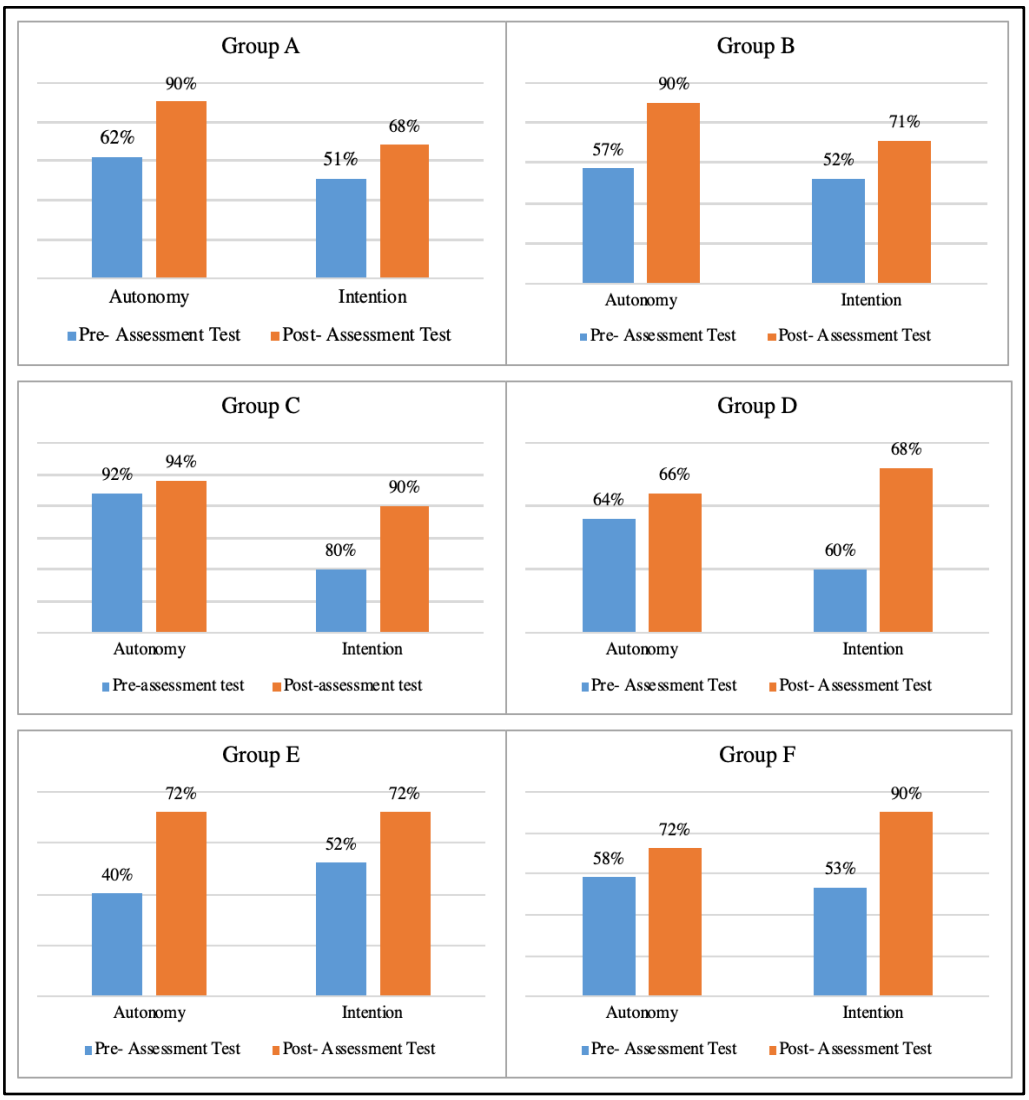

Figure 4. *Mean values from individual assessment tests for all groups*

Table 3. *Pre-assessment results*

	Cyber-Attack, threats and social engineering	E-mail & Internet	Incidents Response	Policies Compliance	Dimensions
Autonomy	56%	65%	57%	57%	59%
Intention	61%	52%	61%	58%	58%
Focus Area	58%	58%	59%	57%	

Table 4. *Post-assessment results*

	Cyber-Attack, threats and social engineering	E-mail & Internet	Incidents Response	Policies Compliance	Dimensions
Autonomy	80%	84%	81%	81%	82%
Intention	82%	72%	76%	74%	76%
Focus Area	81%	78%	78%	77%	

6.4 The Use of the Game Defences for Qualitative Analysis of Intrinsic Motivation

Table 5 shows the investments or defences all groups selected during the game. These investments are described in detail in section 3.2. We used their choices of investments to analyse the autonomy intrinsic factor during the game according to the factor requirements as explained in Section 4. For example, as can be seen in Table 5, for Group A, in game round 1, the players made the decision to choose a firewall, an asset audit and antivirus software to defend against potential threats. We reviewed whether each member in the group contributed to this decision without pressure or control from another member. Also, we checked whether their decision prevented any attacks, and what were the effects of undefended attacks.

Table 5. *Detailed investments by all teams*

Group ID	Round 1	Round 2	Round 3	Round 4
A	-Firewall – Office -Asset Audit -Antivirus	-CCTV – Office -CCTV – Plant	-Threat Assessment -Upgrade – PCs -Upgrade – Servers and Databases -Upgrade – Controller	-Encryption – Databases -Encryption – PCs -Monitoring – Office
B	-Firewall – Office -Firewall – Plant -Asset Audit	-Threat Assessment -Encryption – Databases -Upgrade – Servers and Databases -Upgrade – PCs	-CCTV – Plant -Security Training -Antivirus	-Network Monitor – Plant -Upgrade – Controller -Encryption – PCs

Continued on the next page

Continuation of Table 5

Group ID	Round 1	Round 2	Round 3	Round 4
C	-Firewall – Office -Firewall – Plant -Antivirus	-CCTV – Office -Security Training -Asset Audit	-Encryption – Databases -Upgrade – Controller -Encryption – PCs -Upgrade – PCs	-Threat Assessment -Upgrade – Servers and Databases -CCTV – Plant
D	-Firewall – Office -Firewall – Plant -Antivirus	-Asset Audit -Upgrade – PCs -Upgrade – Servers and Databases -Threat Assessment	-Security Training -Monitoring – Office -Encryption – PCs	-Encryption – Databases -CCTV – Office -Upgrade – Controller
E	-Asset Audit -Upgrade – PCs -Firewall – Office	-Firewall – Plant -Security Training -Threat Assessment -Upgrade – Servers and Databases	-Antivirus -Encryption – Databases -Encryption – PCs -Upgrade – Controller	-CCTV – Office -Monitoring – Office
F	-CCTV – Plant -Monitoring – Plant	-Firewall – Office -Asset Audit -Firewall – Plant	-Threat Assessment -Encryption – Databases -Encryption – PCs -Upgrade – PCs	-Security Training -Upgrade – Servers and Databases -Antivirus -Upgrade – Controller

End of Table 5

6.5 Qualitative Analysis of Autonomy Motivator

6.5.1 Pre-assessment test

Before the game, we assessed each player's autonomy level through a paper-based assessment test. As can be seen in Figure 4, the autonomy levels for Groups A and D were at the average level of 62% and 64% and Group C was at the good level of 92%. In contrast, Groups B, E and F were at the poor level of 57%, 40% and 58% across three awareness focus areas (cyber- attack, threats and social engineering; incident response; and policy compliance) as shown in Figures 4. That means the players needed to improve their awareness levels across these areas.

6.5.2 During the game

We noted during the first round that the average time taken by all six groups to choose the proper defences to build a secure infrastructure for the company was about 40 minutes. On

the other hand, they took only about 15 to 20 minutes in each of the next three rounds because they had become familiar with the security defence types.

It's similar to a real-world workplace: an employee usually spends some time getting to understand a new system with a different interface; after that, they may get used to it or complain about it. It has been determined in numerous studies that an essential feature of ISP development is users' tendency to resist change. In fact, users resist changes of almost all new technologies, guidelines and procedures which require them to act in unfamiliar ways, even when the change is made with the intent of protecting their organisations' information assets [19]. Thus, the organisation should provide a suitable technique for all employees to help them to comply with the new technologies by considering their ideas and opinions about the previous and new technologies.

In the beginning of the game, players in all groups had different security decisions about what to invest in, e.g. a firewall to secure the company network. In the end, they reached a consensus for each decision they made. For example, as shown in Table 5, Group A's members in game round 1 made their own decision to choose firewall, asset audit and antivirus. As a result of their decisions, no visible effect was identified for round one. The GM used software to control the game and created a convincing story after each round to tell the players about the consequences of their decisions so they could know whether their decisions prevented any attacks and the effects of undefended attacks, as in the following example of Group A, game round one.

Defence decision 1, Firewall: It prevents Scanning Kiddie threats because "the office firewall intercepts a number of scanning attempts from all over the world. Apparently, there are people out there very interested in knowing more about your office network" [13].

Defence decision 2, Asset audit: "During the asset audit, an unsecured, undocumented Wi-Fi network was found in the plant. After some investigation, it was learned this was set up years ago by an engineer who is now retired. They needed to install a set of additional debit sensors on the water stream, and an open Wi-Fi network was a cheap and simple solution compared to deploying a complicated set of cables. The Wi-Fi network was never documented and eventually forgotten. It has now been secured with a strong password" [13].

Defence decision 3, Antivirus: "Upon an employee opening an attachment from an unknown sender, the antivirus fires an alert and announces that a malicious program has been stopped from running on the computer. Upon closer inspection, it was indeed a common piece of malware the antivirus stopped just in time: disaster averted!" [13]. Based on the attack narratives after each round, the players learn from their previous decisions and spend more time in the next round discussing investments to enhance the security infrastructure by making proper decisions.

Another example of autonomy support during the game is security-training defence. As shown in Table 5 most of the groups decided to invest in security training to enhance employees' security knowledge. For instance, Group C members made their decision by consensus to choose training topics based on the current security situation of round one to prevent phishing attacks. They discussed how to secure the email and web servers by providing intensive training to avoid employees clicking on random links while browsing the Web or opening email attachments from unknown sources. Thus, the security awareness focus area (cyber-attack, threats and social engineering) increased sharply from a poor level of 56% in the pre- assessment test (cf. Table 3) to a good level of 80% in the post assessment test (cf. Table 4). Also, the use of email and internet awareness focus areas improved from an average level of 65% in the pre-assessment test (cf. Table 3) to a good level of 84% in the post assessment test (cf. Table 4).

These results support autonomy in the shape of providing ideas and opinions and discovering and assessing the player's own cyber security culture. The common factor that was observed for all groups during the game was that each player provided his/her ideas and view-points without control or pressure from other group members.

6.5.3 Post-assessment test

After the game, we assessed each player's autonomy level through a paper-based assessment test. Figure 4 shows that the autonomy level for all groups improved sharply from 62%, 57%, 92%, 64% and 40% in the pre-test to 90%, 90%, 94%, 66%, 72% and 72% in the post-test. This was primarily a result of the D-D game which provided an intuitive environment where all players debated and reached a consensus for each security decision they made.

6.5.4 The overall results of autonomy for all groups

The overall results of autonomy for all groups are shown in Tables 3 and 4. In the pre-assessment test, the main problem with autonomy is that the players did not have the required security awareness knowledge to take the appropriate decisions to prevent specific cyber- attacks or social engineering on the given scenarios-based assessment questions as shown in Table 3. Also, based on their pre-assessment test answers, we found that they have poor knowledge about how to make the right decisions in relation to specific security incidents and ISP compliance to protect the organisation's technology assets and information.

In contrast, Table 4 shows that autonomy improved sharply from 59% to 82% in the post- assessment test. This result is in line with the main purpose of the D-D game, which is to increase players' ability to choose from different defence options to respond to a number of potential threats, known vulnerabilities of the infrastructure, and past and ongoing cyber- attacks.

As stated earlier, autonomy focuses on the desire to protect an individual's scope for action and decision-making. Autonomy was supported during the game, as players could debate and reach a consensus for each decision their group made. Hence, this study demonstrated that the D-D game can play an important role in enhancing a participant's security awareness knowledge across different security issues.

6.6 Behavioural Intention

To assess ISP compliance, we include behavioural intentions only in pre- and post-assessment tests because they play a role in influencing behaviour. Also, this paper research model (See Figure 1) shows that autonomy influences behavioural intention, but we don't know how strongly it feeds into actual behaviour, independently of intention. Since the main goal of this paper is to enhance compliance via the autonomy intrinsic factor, we assessed autonomy through the pre-assessment test, during the game and through the post-assessment test to see whether playing the game influenced behavioural intentions to comply with an ISP. The intention dimension measures the behavioural intention to protect their organisation's information and technology resources through all four security focus areas.

Before the game, we assessed each player's intention level through a paper-based assessment test. As can be seen in Figure 4 the intention levels for Groups A, B, E and F were at the poor level of 51%, 52%, 52% and 53%. That means action would be needed to increase their security knowledge in two security focus areas (the use of email and internet and policy compliance) as shown in Table 3.

On the other hand, Figure 4 shows that Group C had the highest score of 80% among all groups, which means the group members had a good level of intention across all security focus areas; and Group D (Figure 4) was at the average level of 60%, which requires potential action for this group to increase their security awareness knowledge.

After the game, we assessed each player's intention level through a paper-based assessment test. Figure 4 shows that the intention level increased for all groups. The players' behavioural intention level increased sharply from the poor level of 58% (cf. Table 3) to the average level of 76% in the post-assessment test (cf. Table 4). Also, the cyber-attack awareness focus area raised sharply from a poor level of 61% in the pre-assessment

test (cf. Table 3) to the good level of 82% in the post-assessment test (cf. Table 4). That was a primary result of the influence of autonomy on the players' behavioural intentions.

Based on the definition of intrinsic motivation, which refers to doing something because it is enjoyable, we asked participants whether they enjoyed the game activities. It's interesting to note that all 30 participants in this study enjoyed the D-D game as shown in section 10.

Regarding the quality of players' behaviour, we examined the level of movement of the behaviour from control to autonomous according to the degree the ISPs were internalised. The internalisation process involved incorporation of the significance of external or social regulations by individual employees into their personal values [20]. The internalisation process enables the employee to accept a task that does not directly affect his interests. It allows movement along the continuum from controlled behaviour to more autonomous behaviour [21]. This study found that the quality of players' behaviour is self-determined, which means they had high autonomous motivation because they enjoyed and got inherent satisfaction from playing the game.

6.7 Statistical Significance Test

We ran t-test to assess whether there was a statistically significant increase in assessment test scores of the participants after the D-D game play activities.

Table 6 shows the paired sample t-test results conducted for all participants. According to the results, p values of autonomy (t= 5.84, p=0.000), and intention (t=3.84, p=0.000) are less than 0.05, which indicates that post-assessment test results for these factors are significantly greater than pre- assessment test results. Therefore, when we consider all participants, we can conclude that scores of assessment tests for the factors autonomy and intention of the participants improved significantly after they experienced the D-D game.

Table 6. *Overall results of pairwise T-test for all participants*

Factor	T-value	P-value	Significant?
Autonomy	5.84	0.000**	Yes
Intention	3.84	0.000**	Yes

*Significant level: ***p < 0.01, **p < 0.05, *p < 0.1*

According to the findings of this study, the organisation needs to consider their employees as important elements in the information security management framework by motivating but not controlling them towards ISP compliance to reduce security incidents and limit the damage of policy violations. This can be achieved through effective, attractive and proper information security awareness techniques that focus on employees' security behaviour. For instance, an organisation could turn boring, serious company-related rules and regulations into an "affinity" approach that employees are more comfortable with, and present them in the form of interesting game. In the early stage, the organisation should start with an online or internal assessment methods to find weak points in the information security awareness of employees, and targeted communication plans could be formulated. At the same time, it can evaluate and review the results after publicity work about ISP compliance has continued for some time [22]. Hence, the organisation will ensure that employees do not create expensive, unintentional mistakes concerning information security. Also, the employees will have a good understanding of their ISPs and procedures, and they can convey the importance of information security for organisations during the year [23][24][25].

7 Limitations, Future work and Concluding Remarks

As mentioned earlier, the participants in this study were from the University of Glasgow. We did not have permission to observe participants' post-game activities to find out whether playing the game had a positive impact on their actual security behaviour. Future work may consider conducting the study with full-time employees in a real-world work environment to confirm the findings of this study.

In conclusion, this empirical study makes important contributions by providing evidence that security awareness knowledge in the shape of the autonomy intrinsic motivator has an important role to play in reinforcing compliance with ISPs through effective and attractive techniques like the D-D game. This study describes the development of information security compliance assessment methods. Our assessment method's use of a simple data gathering process and specific multi-criteria problem-solving methods delivers a quantitative assessment of information security compliance. The assessment method is scientifically valid, and it may be used as a basis for a more comprehensive and sophisticated assessing system. The results show that the D-D game had a positive effect on the players' autonomy factor, which in turn had a positive effect on their behavioural intention to comply with an ISP (cf. Figure 1). Also, we ran t-test to assess whether there was a statistically significant improvement in participant test scores after they played the D-D game. We found that improvements in autonomy and behavioural intention were statistically significant.

References

[1] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," MIS quarterly, vol. 34, no. 3, pp. 523-548, 2010. https://doi.org/10.2307/25750690

[2] Q. Hu, Z. Xu, T. Dinev, and H. Ling, "Does deterrence work in reducing information security policy abuse by employees?" Commun. ACM, vol. 54, no. 6, pp. 54-60, 2011. https://doi.org/10.1145/1953122.1953142

[3] C.Z.Liu, H.Zafar, and Y.A.Au, "Rethinking FS-ISAC: An IT security information sharing network model for the financial services sector," Communications of the Association for Information Systems, vol. 34, no. 1, p. 2, 2014. https://doi.org/10.17705/1CAIS.03402

[4] R. B. Cialdini and M. R. Trost, "Social influence: Social norms, conformity and compliance." 1998.

[5] J. Leach, "Improving user security behaviour," Computers & Security, vol. 22, no. 8, pp. 685-692, 2003. https://doi.org/10.1016/S0167-4048(03)00007-5

[6] R. M. Ryan and E. L. Deci, "Intrinsic and extrinsic motivations: Classic definitions and new directions," Contemporary educational psychology, vol. 25, no. 1, pp. 54-67, 2000. https://doi.org/10.1006/ceps.1999.1020

[7] J.-Y. Son, "Out of fear or desire? toward a better understanding of employees' motivation to follow is security policies," Information & Management, vol. 48, no. 7, pp. 296-302, 2011.https://doi.org/10.1016/j.im.2011.07.002

[8] M. Vansteenkiste, C. P. Niemiec, and B. Soenens, "The development of the five mini-theories of self-determination theory: An historical overview, emerging trends, and future directions," in the decade ahead: Theoretical perspectives on motivation and achievement. Emerald Group Publishing Limited, 2010, pp. 105-165. https://doi.org/10.1108/S0749-7423(2010)000016A007

[9] M. E. Thomson and R. von Solms, "Information security awareness: educating your users effectively," Information management & computer security, vol. 6, no. 4, pp. 167- 173, 1998. https://doi.org/10.1108/09685229810227649

[10] P. Puhakainen and R. Ahonen, "Design theory for information security awareness," 2006.

[11] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," Information Systems Research, vol. 20, no. 1, pp. 79-98, 2009. https://doi.org/10.1287/isre.1070.0160

[12] S. Frey, A. Rashid, P.Anthonysamy, M. Pinto-Albuquerque, and S. A. Naqvi, "The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game," IEEE Transactions on Software Engineering, 2017. https://doi.org/10.1145/3180155.3182549
[13] R. Awais and B. Shreeve, "Decisions & Disruptions," p. 98, 2017. [Online]. Available: https://sites.google.com/view/decisions-disruptions/
[14] A. Alzahrani, C. Johnson, and S. Altamimi, "Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation," In 2018 4th International Conference on Information Management (ICIM) 2018 May 25 (pp. 125-132). IEEE. https://doi.org/10.1109/INFOMAN.2018.8392822
[15] E. L. Deci and R. M. Ryan, "Hedonia, eudaimonia, and well-being: an introduction," J. Happiness Stud., vol. 9, no. 1, pp. 1–11, Jan. 2008. https://doi.org/10.1007/s10902-006-9018-1
[16] J. W. Adie, J. L. Duda, and N. Ntoumanis, "Perceived coach-autonomy support, basic need satisfaction and the well-and ill-being of elite youth soccer players: A longitudinal investigation," Psychology of Sport and Exercise, vol. 13, no. 1, pp. 51-59, 2012. https://doi.org/10.1016/j.psychsport.2011.07.008
[17] J. D. Wall, P. Palvia, and P. B. Lowry, "Control-related motivations and information security policy compliance: The role of autonomy and efficacy," Journal of Information Privacy and Security, vol. 9, no. 4, pp. 52-79, 2013. https://doi.org/10.1080/15536548.2013.10845690
[18] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," computers & security, vol. 25, no. 4, pp. 289-296, 2006. https://doi.org/10.1016/j.cose.2006.02.008
[19] K. Joshi, "A model of users' perspective on change: the case of information systems technology implementation," MIS quarterly, pp. 229-242, 1991. https://doi.org/10.2307/249384
[20] G. Roth, Y. Kanat-Maymon, and U. Bibi, "Prevention of school bullying: The important role of autonomy supportive teaching and internalization of pro-social values," British Journal of Educational Psychology, vol. 81, no. 4, pp. 654-666, 2011. https://doi.org/10.1348/2044-8279.002003
[21] A. H. Olafsen, H. Halvari, J. Forest, and E. L. Deci, "Show them the money? the role of pay, managerial need support, and justice in a self-determination theory model of intrinsic work motivation," Scandinavian journal of psychology, vol. 56, no. 4, pp. 447- 457, 2015. https://doi.org/10.1111/sjop.12211
[22] M. Karjalainen and M. Siponen, "Toward a new meta-theory for designing information systems (IS) security training approaches," Journal of the Association for Information Systems, vol. 12, no. 8, pp. 518-555, 2011. https://doi.org/10.17705/1jais.00274
[23] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: an action research study," MIS quarterly, pp. 757-778, 2010. https://doi.org/10.2307/25750704
[24] A. Vance, M. Siponen, and S. Pahnila, "Motivating is security compliance: insights from habit and protection motivation theory," Information & Management, vol. 49, no. 3-4, pp. 190-198, 2012. https://doi.org/10.1016/j.im.2012.04.002
[25] C. Brodie, The Importance of Security Awareness Training. Citeseer, 2008.

8 Appendix A (Attacks table)

Table 7. *Attacks targeting the infrastructure and the corresponding counters (defences) noted X in the table -adapted from [12].*

Attacker	Round 1	Round 2	Round 3	Round 4
Scanning Kiddie	Scan offices X Firewall offices	Scan offices X Firewall offices	Scan offices X Firewall offices	Scan offices X Firewall offices
Scanning Kiddie		DoS offices X Firewall offices	DoS offices X Firewall offices	DoS offices X Firewall offices
Hacking Kiddie		Remote control server X Server patch	Data exfiltration server X Net. mon. offices X Encryption DB	Data exfiltration server X Net. mon. offices X Encryption DB
Phishing Kiddie	Phishing offices (Trojan) X Training X Antivirus X Patches PCs	Phishing offices (Trojan) X Training X Antivirus X Patches PCs	Phishing offices (Trojan) X Training X Antivirus X Patches PCs	Phishing offices (Trojan) X Training X Antivirus X Patches PCs
Malware Kiddie		Disruption PC offices X Training X Antivirus X Patches PCs	Disruption PC offices X Training X Antivirus X Patches PCs	Disruption PC offices X Training X Antivirus X Patches PCs
APT PC Offices	Infected USB offices X Training X Antivirus	Remote Control PC X Antivirus X Net. mon. offices	Data exfiltration PC X Antivirus X Encryption PCs X Net. mon. offices	Data exfiltration PC X Antivirus X Encryption PCs X Net. mon. offices
APT Server Offices	Phishing office credentials X Training	Remote Control Server X Net. mon. offices	Data exfiltration DB X Net. mon. offices X Encryption DB	Data exfiltration DB X Net. mon. offices X Encryption DB
APT DB Plant	Vulnerable Wi-Fi plant X Asset Audit	Remote Control DB plant X Patch server X Net. mon. plant	Data exfiltration DB plant X Net. mon. plant X Encryption DB	Data exfiltration DB plant X Net. mon. plant X Encryption DB
APT Controller	Scan plant X Firewall plant	Remote control Controller X Patch controller X Firewall plant	Disruption controller X Patch controller	Disruption controller X Patch controller
State Intelligence	Physical intrusion plant X CCTV plant	0day DB plant X Net. mon. plant	Data exfiltration DB plant X Net. mon. plant	Data exfiltration DB plant X Net. mon. plant
State Disruption	Physical intrusion plant X CCTV plant		Remote control controller (0day)	Disruption controller

9 Appendix B: Assessment Questionnaire

9.1 Example question to test autonomy

You have received an email from an unknown sender asking you to click on the link and provide your email address, phone number, residential address, and credit card info to get coupon points amounting to a 90% discount on branded clothes for shopping at Amazon. What should you do?
A. You will click on the link and share the details
B. You will click on the link, but you will not share the details.
C. You will ignore the email and delete it since it could be a phishing mail. (Correct Answer)
D. You will share that email with your friends to get the coupon discounts since you do not want to use it.
E. I don't know what to do.

Goal: Autonomy focuses on the desire to protect an individual's scope for action and decision-making. This scenario finds out whether the employee would fall victim to a phishing attack. The end-user must make his own decision against this attack, so we observe the employee's level of autonomy. This scenario targets the following awareness focus areas: cyber-attack, the use of email and internet, and policy compliance.

9.2 Example question to test intention

You are getting a reminder for password expiry on your office laptop. How do you create and formalise your password?
A. You will create a password with five lower case letters
B. You will use only six digits
C. You will follow the password policy. (Correct Answer)
D. You will write one of your family member's name and date of birth as a password.
E. I don't know.

Goal: Intention refers to an employees' intention to protect their organisation's information and technology resources. This scenario finds out whether the employee intends to comply with the password policy. It also tests his/her awareness of related policies. This scenario targets one awareness focus area: policy compliance.

10 Appendix C (Participants' profile)

Table 8. *Demographic characteristics of the sample*

Variable	Frequency	Percent (%)
Gender		
Men	19	63.33
Women	11	36.67
Highest Level of Education		
High School	0	0
Diploma	0	0
Bachelor's	4	13.33
Master's	26	86.67
PhD	0	0
Other	0	0
Years of Computer Use		
Less than One Year	0	0
1–2 Years	0	0
3–4 Years	0	0
5–6 Years	6	20
More than 6 Years	24	80
Years of Internet Use		
Less than One Year	0	0
1–2 Years	0	0
3–4 Years	7	23.33
5–6 Years	23	76.67
More than 6 Years	0	
How Would You Rate Your Overall Proficiency in Information Security Awareness?		
No Particular Training	2	6.67
Some Technical Knowledge	23	76.67
Significant Training or Experience	2	6.67
Expert	3	10

After the Game	Frequency	Percent (%)
Did You Enjoy the Game?		
Yes	30	100
No	0	0