Developing a Simulated Intelligent Instrument to Measure User Behavior toward Cybersecurity Policies

Khalid Adnan Alissa[1], Bashar A. AlDeeb[2], Hanan A. Alshehri[1], Shahad A. Dahdouh[1], Basstaa M. Alsubaie[1], Afnan M. Alghamdi[1] and Mutasem K. Alsmadi[3]

[1]College of Computer Science and Information Technology, Imam Abdulrahman bin Faisal University, P.O. Box 1982, 31441, City of Dammam, Saudi Arabia.
[2]Deanship of Information and Communication Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, 31441, City of Dammam, Saudi Arabia.
[3]Department of MIS, College of Applied Studies and Community Service, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, 31441, City of Dammam, Saudi Arabia.

Abstract: Since the science of computer networks began, their use has increased and thus the need for it has increased in all areas of life until it has become a necessity. On the other hand, there are some risks that threaten institutions that rely on networks, especially when using the Internet. So, Institutions struggle to protect themselves from threats and cybercrime. Therefore, they devote much attention to improving information security infrastructures. Users' behaviors were explored via a traditional questionnaire research instrument in a data collocate process. The questionnaire explores users' behaviors theoretically, so the respondents' answers to the questionnaire are insufficiently reliable, and the responses might not reflect actual behavior based on the human bias when facing theoretical problems. This study aims to solve unreliable responses to the questionnaire by developing a simulated intelligent instrument to measure users' behaviors toward cybersecurity policies in an experimental study using gamification.

Keywords: Computer Networks, Cybersecurity, Intelligent instrument and User behavior.

1. Introduction

Organizations make great efforts to protect their network and information security infrastructure from significant threats and security risks [1, 17, 18, 19]. Concentrating on technical solutions to cybersecurity often fails to acknowledge efficient systems, because users must understand and engage with the network and cybersecurity systems [2]. Several studies show that the weakened element in the cybersecurity chain is the end-user [1, 3]. Unfavorable engagement aspects, risky cybersecurity behaviors, and misdirected attention can all increase organizational susceptibility to security deficiencies [2]. User behavior toward the implementation of cybersecurity policies is important in protecting organizations from risks.

Humans are considered a threat source, and humans can cause dangerous events. However, controls and security policies can mitigate threat sources [4]. User behavior is defined as activities performed by individuals, and it varies from one user to another. Therefore, predicting specific patterns of use for all users is difficult because each user behaves differently. Furthermore, users are the weak connection in the information security system [5]. User behaviors might yield security threats and corrupt information security (IS) systems, infrastructure, and software. Understanding how users think and behave (to curb wrong behaviors) is difficult. To prevent wrong behaviors, organizations should apply security controls (procedures and policies). Security systems might protect users from malicious attacks, but procedures and policies must be followed to ensure that users will not make mistakes that could cause system threats [5].

In previous studies, users' behaviors were explored via a traditional questionnaire research instrument in a data collocate process. However, the questionnaire has weaknesses in human behavior studies. Using questionnaires to collect required data about user behaviors will reveal weaknesses theoretically. Therefore, these points can be handled more easily, and users' behavior and performance may be theoretically improved to the required level. However, many researchers studied the reliability of the respondents' answers to the questionnaire and found that respondents sometimes answered questions inaccurately—not reflecting actual behavior (based on the human bias) when facing theoretical problems.

In addition, establishing a network and information security infrastructure is very important for all institutions. Thus, we have tried to make respondents answer the questionnaire using an intelligent method that reflects and mimics actual behavior.

In the last decade, simulation technology has become an effective method in many fields (education, training, playing, etc.) and has found great success in all fields where it has been used. Therefore, researchers use simulation-using games to find the actual behavior of users.

The previous studies [6-9] illustrate how to use online games to measure the behavior of individuals (players) through their movements and reactions before, during, and after the game. It is considered a powerful addition to online games when used appropriately. In general, behaviors differ from one human to another, so they are hard to understand. However, organizations face various human behavior patterns, so organizations must apply a security policy to protect assets from these differences. These security policies enforced by the organization need compliance regardless of difficulties and obstacles. Moreover, some organizations tend to use online games to measure employees' behaviors for further analysis.

Businesses should use various cybersecurity measures to protect their business data, cash flow, and customers online. These measures should prevent risks from different sources, which include:

- Internet-borne attacks (e.g., spyware or malware),
- User-generated weaknesses (e.g., easily guessed password or misplaced information),

- Inherent system or software flaws and vulnerabilities, and User-generated weaknesses are a priority for organizations.

Therefore, organizations set policies for users to follow in order to secure information. These policies can be defined as a set of rules and laws used to deal with the information and the various techniques within the organization. These rules and laws illustrate what is permitted and what is unauthorized. On the other hand, they also define mechanisms via statements by which information is accessed and managed. So, these policies concern security solutions for all transactions but do not engineer and formulate the solutions.

Rees, Bandyopadhyay [10] defined security policy as generally high-level, concern risks, technology-neutral set procedures, and directions, and define countermeasures and penalties if the policy is transgressed and must not be confused with implementation-specific information, which would be part of the security procedures, standards, and guidelines". These standards, guidelines, and procedures are fundamental for protecting the institution by protecting data confidentiality, integrity, and availability [10].

- "Confidentiality: protect information from disclosure and restrict access to information through authorized user only" [13].
- "Integrity: ensure the completeness and accuracy of the information and prevent any unauthorized conduct such as modification and deletion" [13].
- "Availability: Ensure that information and services are available to the authorized user wherever and whenever necessary" [13].

These objectives are an integrated model for policy guidance to support and protect organizations.

Attacks are increasing significantly, and this results in increasing the risk of damage to organizations [11]. This menace motivates organizations to add more security mechanisms to reduce the number of successful attacks and, consequently the damage due to security breaches [11].

Many information security specialists agree that if the organization promotes good behaviors and constrains bad behaviors, it will make information security within the organizations more efficient [12].

Human behavior is defined as a person's actions or conducts [5]. Human behavior from an IT perspective is the same. It is defined as "actions made by individuals when they use computers or in other words human interactions with computers" [5].

In the computer science understanding field, human behavior is considered a complex problem because the behavior is usually unexpected. Controlling human behavior related to information security is important to maintain the security of all systems and applying a control mechanism on human behavior guarantees information security [13]. Human behaviors are hard to predict, so control mechanisms must be restricted to protect the organization from possible risks [14]. Humans are considered one threat source, and humans can cause dangerous events. However, controls and security policies can mitigate threat sources [4]. User behavior is defined as activities carried out by individuals, and it varies from user to another. Therefore, predicting specific patterns of use for all users is difficult because each user behaves differently. Furthermore, users are the weak connection in the information security system. Users' behavior might yield security threats and corrupt IS systems, infrastructure, and software. It is difficult to understand how users think and behave in order to curb wrong behaviors. To prevent wrong behavior, organizations should apply security controls (procedures and policies). Security systems might protect users from malicious attacks, but they must connect with procedures and policies to ensure that users will not make mistakes that threaten systems.

User behaviors were measured by applying a traditional questionnaire as a research instrument in the data collocate process. Complex human behavior is difficult to measure with a valid and reliable instrument. The instrument considers the underestimation of a human brain's ability to measure the complexity of its behavior via an imaginary situation. The questionnaire explores user behavior theoretically, so the respondent's answers to the questionnaire are insufficiently reliable, and the responses might not reflect actual behavior (based on human bias) when facing the theoretical problems. Therefore, a valid and reliable instrument is required to measure behavior in a way similar to real life.

Measuring human behavior toward security policies with a reliable instrument is this study's main problem because it is a key factor for companies, institutions, and all sectors trying to strengthen behaviors toward strong security policies. Bad behaviors affect the environment, so the measurement primarily builds a safe game environment where individuals can behave naturally. The current study's main aim is to create a simulated intelligent instrument to measure user behaviors toward cybersecurity policies in an experimental study using gamification.

2. Related Work

Several studies in the past 15 years have used computer games to investigate basic behavioral processes in humans. Scholars who concentrate on information security trust that improving the compliance of end-user behaviors and restraining bad end-user behaviors will improve the efficiency of information security within the institutions [12].

Researchers assessed users' behaviors in the context of policies. For example, Stanton, Stam [12] conducted a study on several industry employees in the United States. The study explores the influence of end-user behavior on the efficiency of security in the industries. This study found six measurements concerning security behavior, which were assorted into two long measurements: technical expertise and intentionality. The first measurement classified behaviors as intentionally beneficial, intentionally malicious, or lacking a straightforward intention. The second measurements assess the information technology knowledge and skills desirable for applying the described behavior. The six-security behavior element concerned password selection and password-changing frequency [5]. The study recommended improving users' behaviors to benefit the organization by increasing staff awareness of the policies and of the importance of implementing them and by urging employees to adhere to the stated policies [12].

In 2007, Pahnila defined security policy generally as a set of laws and rules used to deal with the information. The various techniques within the organization explain what is prohibited and what is permitted. On the other hand, security policy defines its mechanisms via statements about accessing and managing information. So, it concerns security solutions for

all transactions but not how to engineer and formulate these solutions. A study on a Finnish company used a "seven-point Likert" scale [15]. It was a web-based questionnaire for measuring the factors, the study suggests that one factor that significantly affects IS compliance: information quality. The factors of employees' attitude habits and normative beliefs also have significant effects on the intention to comply with IS, while facilitating condition and threat appraisal significantly impact IS policy compliance. Furthermore, coping appraisals do not have a significant effect on employees' attitudes toward complying, and sanctions have a nominal effect on intentions to comply with IS policy. [15].

Most studies have concluded that cybersecurity in institutions is affected by security errors caused by human behavior. Studies have also shown that institution's success in protecting their information security depends on individuals' skills, knowledge, and awareness regarding cybersecurity aspects [16]. Most previous studies also included some suggestions and recommendations, including that institutions must have a framework for assessing human reliability, tools and systems for monitoring user behaviors, and a system for scoring cybersecurity's human vulnerability [16].

3. Experimental Setup

This section discusses and summarizes the methodology provided to achieve the study objectives. Mainly, researchers suggested using gamification to build an intelligent instrument by exploring and eliciting user behaviors toward cybersecurity policies. They conducted five stages as shown in figure 1.

Stage 1: Identify cybersecurity measures to use in this study that maintains users' confidentiality and privacy.

Stage 2: Select the appropriate policies for each cybersecurity measure.

Stage 3: Identify survey paragraphs for each measure that determine users' commitment to cybersecurity policies.

Stage 4: Transform all questions into scenarios. Each scenario may cover one or more questions depending on the largest collection of answers from the user to ensure that the answer is accurate and not randomly answered.

Stage 5: Test the result with the pilot study.

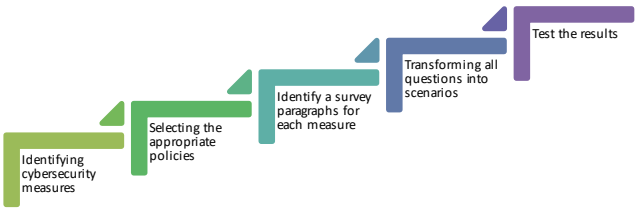

Figure 1. Schema of the Research Methodology.

The following paragraphs will explain the methodology stages in details.

3.1 Identifying cybersecurity measures

Cybersecurity measures were selected based on the most common measures used in institutions like the SANA and SANS institutes and on state-of-art measures [4, 11, 15].

Figure 2 demonstrated common cybersecurity measures used in this study. The first measure is the password, researchers chose this measure because the System Admin, Audit, Network, Security (SANS) Institute used it, they classified the password as a critical element and an important aspect of computer and information security [5].

E-mail is the second measure, it is necessary to provide policies, controls, and guidelines for using e-mail to protect the data used by e-mail [12]. The third measure is identity, relying on Borges, Conci [4] paper that specified how users behave if their identity is lost. Users must keep their identities from being stolen, so policies must be in place to guide users regarding identity protection [4]. Fourth, sensitive information requires procedures and policies to guide users on what to do before the information is stolen or exposed. [13]. The fifth measure is resource/physical security and how humans protect their resources from unauthorized access. This study will use all previous measures of human behavior, policies, and usage guidelines to develop a measure of the user's compliance with these policies [5].

3.2 Policies selection and identifying, alignment with its questions.

In this stage, the researchers describe the policies for each measurement (For policy details, see the extended paper [5]).

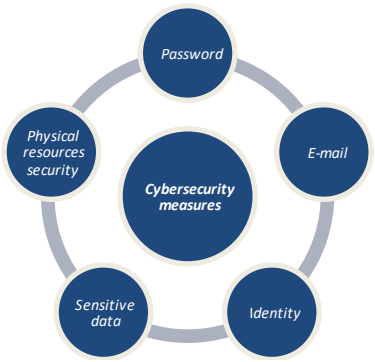

Figure 2. Common Cybersecurity Measures

These policies were brought to cybersecurity experts for validation and arbitration. In the review process, each expert was interviewed separately. The authors considered this feedback to support paper policies in terms of importance in measuring behavior. Thereafter, the instrument was designed on a scientific basis.

3.3 Identify survey paragraphs for each measure that determine users' commitment to cybersecurity policies.

The design of the questionnaire paragraphs was used questionnaires from literature relevant to human behaviors. Then, it was accustomed to fulfil the study requirements. We formulated one or more questions to measure compliance with each policy. Subsequently, the alignment of policies and survey questions were reviewed by the same experts to get their feedback (See table 1). Then, we took the feedback from the experts into account and made amendments according to the experts' opinions. At each stage of the amendment, we showed the result to the experts until a final state was approved by all.

3.4 Transforming all questions into scenarios

In this stage, a traditional survey will become an intelligent survey by transforming each paragraph into a scenario. To be more accurate in measuring human behavior, each user will behave differently. The purpose of this study is to allow individuals to behave as normally as they can, so the intelligent survey must be implemented as consistently as

possible for each simulated question and measure that must be studied. The following section will explain how we implement an intelligent survey as an auxiliary step that supports measuring human behavior towards cybersecurity policies. It will be carried out in a specific process.

As mentioned before, the questions will be transformed into scenarios and implemented in a creative questionnaire. Implementing a creative questionnaire starts with dividing the whole scenario into multiple scenes, and each scene has its characters that play an important role in the scenario. Then, the characters are designed as an animation with a focus on each detail of the character, such as their position, facial expression, office design, and screens to formulate whole scenes. The next step is activating all these scenes via programming languages such as HTML5/CSS and JavaScript. These will all be combined to perform an intelligent survey that will be shown as an interface on the website, it will also include the admin dashboard. The third step is storing players' answers and scores for each question in the database uploaded to the server (using PHP language). This section will review all of these.

3.4.1 Scenario and question

This subsection shows how all the questions were translated into a consistent and complete scenario. Each scenario may cover one or more questions depending on the largest collection of answers from the user to ensure the answer is accurate and not random. Eventually, we ended up with 20 questions as shown in table 1:

3.4.2 Scenes of the Scenario

This subsection illustrates the creative questionnaire and its work mechanism. The creative questionnaire's home page provides access to many other web pages, such as teams and services, which will open an admin dashboard as shown in Figure 3. It also illustrates how the player will interact with the actions in each scene by choosing the age, gender, and region before clicking the "START" button on the home page. The player now can play the game "Answering the questions." The game starts with introducing the main characters presented to the player: the company manager (Jack), the secretary (Kate), a person looking for a job (Mark), and the office colleague (Smith), as shown in Figure 4. Then, each scene will be displayed as a video that automatically plays without the player's intervention. At the end of the video, a web page will be displayed asking the user to deal with the actions. The response will then be stored directly in the database.

Figure 3. Home Page

Figure 4. Main Characters

First scene

Characters: Job seeker and Company secretary.

First, a person sends his resumé to a company asking for a job, as shown in Figure 5. The company secretary receives this resumé, as shown in Figures 6 and 7. Now the secretary has to either open the file and reply (the player gets one point), take extra time to check the resumé file before downloading it (the correct option—he gets three points), or open it later (he gets one point). After each case is discussed above, the secretary will reply to that person with the date and time of the interview.

Figure 5. Person Sending his Resumé and Asking for a Job

Figure 6. Secretary Received the Resumé

Figure 7. Resumé Highlighted Options

Table 1. Transforming survey questions to scenarios.

#	Policy #*	Measurement	Question	Scenario
1	2	E-mail	***Question 1:*** "*What will you do when you receive an e-mail with an attachment?*" [5] (Multiple choice question) ***Answers:*** Open it immediately/ Open it after a virus scan even if it takes more time/ Never open it.	The beginning of the scenario simulates a person sending his CV to a company and asking for a job. The company secretary receives this CV, and the secretary must either open the file and reply (the player gets one point), take more time to check the CV file before downloading it (which is the correct action—he gets three points), or open it later (he gets one point). After each case is discussed above, the secretary will reply to that person with the date and time of the interview.
2	1	Password	***Question 2:*** "*When constructing a password, you should*" [5]: (Multiple choice question) ***Answers:*** 1. Use a family member's name, sports name, and pet name with a number at the end. 2. Use misspelled words or phrases with embedded numbers and special characters. 3. Use sequenced numbers and letters from your keyboard.	The new employee goes to the company for the job interview and is subsequently informed of his acceptance. On the first day of the job, the manager gives the employee a default password so he can complete the electronic form with his data. The manager then tells the employee to change the default password if he wants. While filling out the form, the password field will be shown to the player. He can fill it out or keep the default password. The password strength will be classified as: (Weak, Medium, Strong, and Default password), If the player selects (a), one point will be added to his balance. If he selects (b), he receives two points. If he selects (c), the best answer, three points will be added. If he preferred the default password, he answers another question as shown below.
3	1	Password	***Question 3:*** "*Do you prefer to use the default password?*" [5]. ***Answers:*** Yes/No.	If he chooses to use the default password in Question 2, the result here will be yes. If he selects another answer in Question 2, the result will be no.
4	1	Password	***Question 4:*** "*What is an example of a strong password?*" [5]	This question depends entirely on Question 2. If the player selects (b), his answer will be strong, and he will earn three points in this question. Otherwise, he earns only one point.
5	3	Password	***Question 5***: "*Which one of the following methods can be used to secure your password from disclosure?*" [5] ***Answers:*** Sticky note/In your phone/Memorize it.	After finishes filling out the form, the employee's alerts are displayed to find out where the selected password will be stored. If he memorizes it (c), he gets three points because makes it difficult for anyone to take the password. If he saves it in his phone option (b), he gets two points. If he chooses (a), he gets one point because he leaves it open to everyone.
6	2	Password	***Question 6***: "*What should you do if someone asks you for your password?*" [5] ***Answers:*** Agree/Disagree.	One day, the employee is asked to prepare for the meeting to discuss a new study, and an employee presentation is required to discuss project proposals. The employee begins processing the presentation and is simultaneously asked to send an e-mail containing the weekly report handed over from the department head. He then suggests his colleague in the office send the report on his behalf. These options will appear: • Send the report immediately before going to the meeting. • Ask your colleague to send it to you. • Postpone submitting the report until after the meeting. If the employee sends the e-mail by himself—either immediately or by postponing the submission and apologizing to the department head—the answers for Questions 6 and 7 will be Disagree and No; so, he gets three points. On the other hand, if he requests his colleague to send it instead, the result will be Agree and Yes; so, he gets one point.
7	2	E-mail	***Question 7:*** "*Would you allow a (trusted/untrusted) person to use your e-mail account to send an urgent and important message?*" [5] ***Answers:*** Yes/No.	
8	3, 4, and 5	Sensitive Data	***Question 8:*** "*Do you leave sensitive data in open areas (copiers, faxes, printers, desktops)?*" [5] ***Answers:*** Yes/No.	If the employee allowed his colleague to submit the report in the previous Question 7 scenario, he would give his colleague access to all the sensitive sources on his machine. The answer would be yes (one point). If he did not, the answer is no (three points).
9	1,2,4,5, and 6	Physical/Resources Security	***Question 9:*** *"Do you follow the physical security practices?*" [5] ***Answers:*** Yes/No.	After the meeting, the employee will look at the wall clock and know that official working hours have ended. The employee must turn off his computer and is shown these options: • Shut down the system/Press the power button until the system turns off/Remove the power cable.
10	1, 2, 3, 4, 5, and 6	Physical/Resources Security	***Question 10:*** "*Do you physically secure your computing devices (desktops, laptops, portable drives, and smart devices)?*"[5] ***Answers:*** Yes/No.	The last thing the employee should do before leaving the office is to lock the door. In the displayed scene, the employee is in his car and forgets to lock the office door. Two options will be shown: • Return to lock the door–Yes for Questions 10 and 11. • Maybe my colleague will lock the door–No and No.
11	1,2,4,5, 6, and 7	Physical/Resources Security	***Question 11:*** "*Do you store your sensitive/critical data in a secure area?*" [5]	

			Answers: Yes/No.	If the employee locked the door, then he secured all the computing devices in the office, and all critical data will be in a secure area, so he gets three points. If he misses this step, he gets one point only.
12	1	Identity	***Question 12:*** "*What should you do if someone tries to steal your identity?*" [5] ***Answers:*** 1. Report the issue to the bank/civil status. 2. It is not a problem/ignore it. 3. It is a problem, but you will deal with it later.	The next day, the employee sat in his office and was conversing with his colleague before being summoned by the manager. He left his card and wallet in his office. The colleague exploited the employee's absence and took a picture of the bank card's front and back before returning it. The colleague tries to access the employee's bank account. So, the employee receives a verification code from the bank. If the player reports the issue to the bank in Question 12, then the answers for Questions 13 and 14 will be Yes and Yes. That means the employee reports to the bank that he believes someone tried to access his account (he gets three points). If the player ignores this message in Question 12, the answer to both questions will be No and No. That means he thinks this message has reached him by mistake, and no one is trying to steal his information. Thus, he ignores the message (he gets one point). If he leaves the message because he will deal with it later, the last option, the answers for Questions 13 and 14 will be No and Yes (he gets two points because he believes someone tried to access his account but doesn't report the issue to the bank).
13	2	Identity	***Question 13:*** "*Did you contact a credit bureau about the misuse or attempted misuse of your personal information?*" [5] ***Answers:*** Yes/No.	
14	3 and 4	Identity	***Question 14:*** "*Is there someone tries to access your bank account?*" [5] ***Answers:*** Yes/No.	
15	3	E-mail	***Question 15:*** "*If you received an e-mail message from an online shopping website while using the company's e-mail account, would you respond to that e-mail?*" [5] ***Answers:*** Respond to the e-mail/Ignore the e-mail/Block the source of the e-mail.	At his office, the employee received a marketing e-mail via the company's e-mail. If the employee responds to that e-mail, the results for Questions 15 and 16 will be Respond to the e-mail and Yes. If he responds, he will be directed to another fake page to enter his personal information to register, and he will get one point. If he ignores the e-mail, the results will be Ignore the e-mail and No, so two points will be added to his balance. If he blocks the source of that e-mail, which is the ideal answer, he will earn three points and the answers will be Block the source of the e-mail and No.
16	2	Sensitive Data	***Question 16:*** "*Do you text or post sensitive data on a social site?*" [5] ***Answers:*** Yes/No.	
17	4	E-mail	***Question 17:*** "*Most e-mails are sent in plain text, so they can be intercepted and read online.* *Do you think the e-mail content should be encrypted?*" [5] ***Answers:*** Don't know what encryption is/No need for encryption/Should be encrypted even if it takes more time.	Mark's supervisor asked him to send the credentials report, which contains the company's expense details, as fast as possible. He warns Mark against exposing this information, so he needs to secure it and send it quickly. The three options above will be displayed before he sends the e-mail to the manager. If the player chooses option (a), he gets one point, and the dialogue that contains the encryption definition will be displayed to him. If he chooses option (b), he gains two points in Question 17 and one point in Question 18. If he chooses option (c), he gains three points in Questions 17 and 18, which is the best answer.
18	1	Sensitive Data	***Question 18:*** "*Do you encrypt sensitive data when sending messages via external e-mails?*" [5] ***Answers:*** Yes/No.	
19	7	Physical/Resources Security	***Question 19:*** "*If you have a personal laptop, would you protect it with virus protection and software patches?*" [5] ***Answers:*** Yes/No.	Mark discusses with his colleague about the meeting that took place on the first day. During the meeting, they mentioned the importance of virus protection and software patches that increase information security and offer other advantages. His colleague says "Yes, I have heard about the importance of all these. Then, he asks Mark, "Do you install a virus protection and download the new software updates on your laptop?" If Mark answers yes, Question 19's answer will be Yes, and he gains three points. If he answers no, Question 19's answer will be No, and he gains one point. His colleague also informs Mark that the company policy forces us to back up all our computer data weekly. During this time, we cannot use the computer until the backup process stops. He asks Mark, "You will apply this policy and back up your data or not?" If he said yes, then Question 20's answer will be Yes, so he gains three points. Otherwise, the answer will be No, and he gains one point.
20	1	Sensitive Data	***Question 20:*** "*Do you backup your sensitive/critical data on a routine basis?*" [5] ***Answers:*** Yes/No.	

* To read all policies, see the extended paper [5].

Second scene:

Characters: The employee and Company secretary.

The new employee goes to the company for the job interview and is subsequently informed of his acceptance, as shown in Figure 8. On the first day of the job, the company secretary gives the employee a default password, so he can complete the electronic form with his personal data. The manager then tells the employee to change the default password if he wants, as shown in Figures 10 and 11. While filling out the form, a password field will be shown to the player, so he can fill it out or keep the default password, as shown in Figure 11. The password strength is classified as Weak, Medium, Strong, or Default password.

If the player selects (a), one point will be added to his balance. If he selects (b), two points will be added. If he selects (c), three points will be added, which is the best answer because it is a strong password. If he preferred the default password, no points will be added because it is the default password.

Figure 8. Acceptance for the Job

Figure 9. Secretary gives job requirements

Figure 10. The Default Password

Figure 11. Entering the Password

Third scene

After the employee fills out the form, the employee's alerts are displayed to find out where the selected password will be stored, as shown in Figure 12. If he memorizes it, option (c), he gains three points because this choice makes it difficult for anyone to take this password. This option will be shown to the player as a mind icon. If he saves it in his personal phone, option (b), he gets two points. It will be shown to the player as a mobile phone icon. If he chooses (a), he gets one point because he left it open to everyone.

- Sticky note? /On your phone? /Memorize it?

Fourth Scene

One day, the employee is asked to prepare for the meeting to discuss a new project. An employee presentation is required to discuss project proposals, as shown in Figure 13. He begins processing the presentation and is simultaneously asked to send an e-mail containing the weekly report to the department head. His colleague in the office suggests that he send the report on the employee's behalf, shown in Figure 14. The options will appear as:

a. Send the report immediately before going to the meeting.
b. Ask your colleague to send it to you.
c. Postpone submitting the report until the end of the meeting.

If the employee sends the e-mail by himself—either sending it immediately or postponing the submission and apologizing to the department head—he gains three points. If he requests his colleague to send it instead, he earns one point because he has given his colleague access to all the sensitive sources on his machine. So, one point will be added based on leaving sensitive data unsecured, as shown in Figure 15.

Figure 12. Where to Store the Password

Figure 13. Employee has a Meeting

Figure 14. One of the Fourth Scene Question's Options

Figure 15. The Question Options

Fifth scene

Characters: Employee.

After the meeting, the employee will look at the wall clock and know that the official working hours have ended, as shown in Figure 16. The employee must turn off his computer and will be shown these options:

a. A button that lets the player shut down the system.
b. Push the power button until the system turns off.
c. A cable icon that lets the player remove the power cable.

If the player shut down the system, he followed the security practices and earns three points. If he locks his system,

presses the power button until the system turns off, or removes the power cable, he earns one point, as shown in Figure 17.

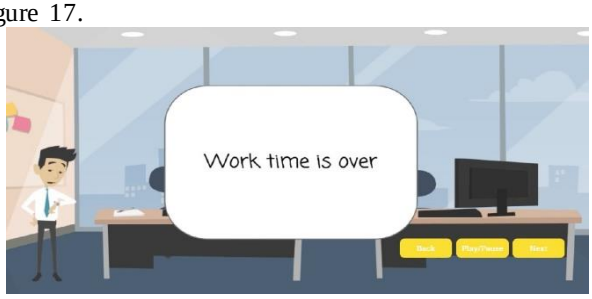

Figure 16. Mark Must Leave his Office

Figure 17. How to Turn Off the PC

Sixth scene

Characters: Employee.

Before leaving the office, the employee should lock the door. In the displayed scene, the employee is in his car and forgot to lock the office's door as shown in Figure 18. Two options will be shown: Return to lock the door or Maybe my colleague will lock the door. If the employee locked the door, he secured all the computing devices in the office, and all the critical data will be in a secure area, so he gets three points. If he misses this step, he gets only one point.

Seventh scene

Characters: Employee, Office colleague. And Manager.

The next day, the employee sat in his office conversing with his colleague when the manager summoned him. He left his card and wallet in his office. The colleague exploited the employee's absence and took a picture of the bank card's front and back before returning it. The colleague tried to access the employee's bank account, so the employee received a verification code from the bank, as shown in Figure 19. The player will be worried about this message, so he has three options to deal with this situation, as shown in Figure 20. If the player reports the issue to the bank, that means the employee believes someone tried to access his account, so he gets three points. If the player ignores this message, that means he thinks the message reached him by mistake, and no one is trying to steal his information. Thus, he ignores the message and gains one point. If he leaves the message to deal with it later, which is the last option, he gets two points because he believes someone tried to access his account but doesn't report the issue to the bank. All the options will appear to the player as an animation.

Figure 18. Mark Forgets to Lock the Office

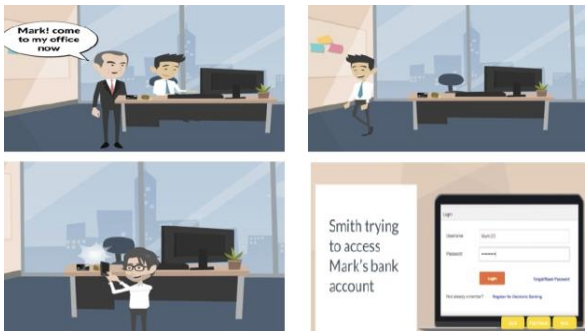

Figure 19. Smith Trying to Access Mark's Account

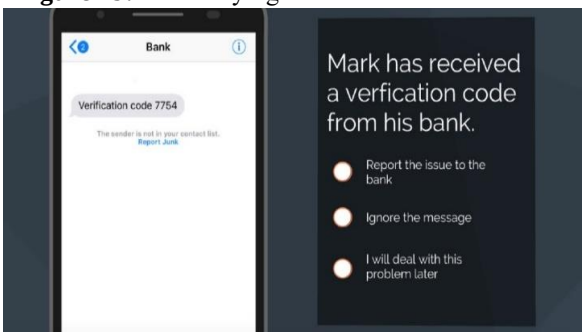

Figure 20. Mark Received a Verification Code

Eighth scene

Characters: Employee.

At his office, the employee received a marketing e-mail via the company's e-mail. The player will see three options with clickable icons on the e-mail screen. One icon is for opening the e-mail, the second one is for blocking the e-mail, and the

Figure 21. Received Marketing E-mail

third is for ignoring the e-mail, as shown in Figure 21. If the employee responds to that e-mail, he will be transferred to another fake page to enter his personal information to register and will get one point. If he ignores the e-mail, two points will be added to his balance. If he blocks the e-mail's source, which is the ideal answer, he will earn three points.

Ninth scene

Characters: Employee and Supervisor.

The employee's supervisor asked him to send the credential report as fast as possible. It contains the company's expense details, and he warns against exposing this information. The employee must secure it and send it quickly. For the three options for securing the e-mail content, the e-mail screen contains three icons: one for taking the time to send it with encryption, one for sending it immediately without encryption, and a third for when the player has no idea about securing the e-mail and doesn't know what the encryption is, as shown in Figure 22. The option will be displayed before sending the e-mail to the manager. If the player chooses the last option, he gains one point, and the contained dialogue (the encryption definition will be displayed to him). If he chooses the second option, he gains two points for not securing the content and one point for not encrypting the

sensitive information. If he chooses the first option, he gains three points for securing the content, which is the best answer.

Tenth scene

Characters: Employee and Office colleague.

The employee discusses with his colleague the meeting that was on the first day. During the meeting, they mentioned the importance of virus protection and software patches which increase information security and offer other advantages. His colleague says "Yes, I have heard about the importance of all these." As shown in Figure 23, he then asks the employee, "Do you install a virus protection and download the new software updates on your laptop?"

If he answers yes, he gets three points. If he answers no, he gets one point. His colleague also informs him that the company policy forces us to back up all the data on our computer weekly. During this time, we cannot use the computer until the backup process stops. As shown in Figure 24, he asks the employee, "You will apply this policy and back up your data or not?" If he said yes, he gets three points. Otherwise, he gets one point. This is the final scene, and after the player completes all scenes, he/she will see the total score. Grades are shown in Figure 25.

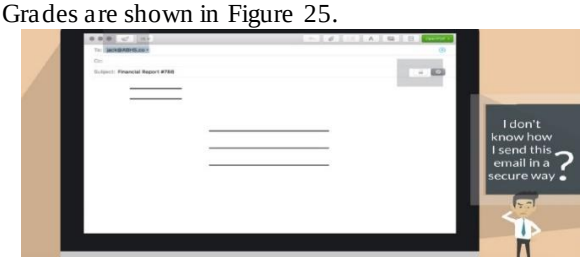

Figure 22. Send E-mails Securely

Figure 23. Virus Protection

Figure 24. Backup Policy

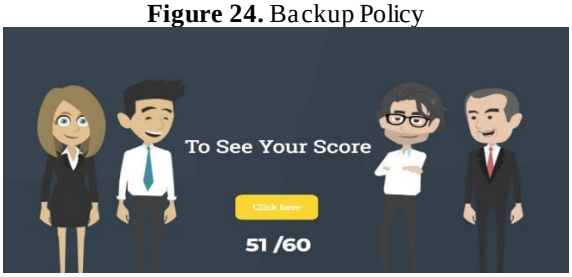

Figure 25. Final Score

All scenes were implemented via HTML5/CSS on several web pages, and all web pages contain actions. These actions are the actual scenes where the player interacts with the icons, buttons, and input fields to provide results. These results are considered the player's answers that will be stored in the database via MySQL queries, which are written in PHP language. JavaScript coding is used to allow the icons, buttons, to be animated and move in a way that encourages the end-user to click on them. It is also used to allow the player to navigate between pages. For example, when the player completes the first scene's web page, it moves to the second scene automatically. Finally, each player has their session to avoid any conflict with other players playing at the same time. To sum up, the above subsections, implementing a creative questionnaire requires testing, review, and distribution among the people to collect a valuable number of samples for further analysis. Testing will include questionnaire testing, a pilot study test, and a user-interface test. These tests will be detailed in the next sections.

3.5 Testing

The creative questionnaire called Traction Game System has been developed to make the process of collecting questionnaire results from end-users more realistic and accurate. This system must be tested via different methodologies to achieve the desired and most accurate results. The process starts with identifying the strategy, criteria, testing methods, specific items to be tested, the testing process, and the testing environment.

3.5.1 Testing Strategy

The strategy includes the characteristics of a basic plan: quality, time, resources, and risk. The plan will focus on detecting differences in the desired and predicted results. It will also evaluate the features in different conditions. The required testing strategy includes components, integration, and system testing, which are clearly defined in the following sections. First, items to be tested and the approaches that will be used are defined.

3.5.2 Test Items

A list of items to be tested will be included. The traction game system will be tested against the system's functional requirements. It has eight modules that will be tested to ensure it satisfies the stated requirements.

The study models include the following: questionnaire test, pilot study test, and user interface test.

3.5.3 Questionnaire Test

This test includes several validity steps to validate the instrument built during this study. An important validity test is "face validity," which will be detailed in the following section (the pilot study). Another type of validity test is "content validity," and this step has been done while building the questionnaire. A panel of experts involved in building and reviewing the instrument's content reached an agreement that the content is valid from their expert point of view.

3.5.4 Pilot Study Test

The pilot study is done by applying and distributing the creative instrument to a small number of people to test the instrument's validity. This study's main point is to ensure that this instrument can be used to assess human behaviors toward the selected cybersecurity policies. This type of study helps build the "face validation" because results from such a test will indicate, for example, if it is easy to continue the whole process. We can decide that by comparing the percentage of the people who completed the whole process to people who stopped in the middle. Moreover, feedback from participants shows how easy it was to understand and follow the steps. Such feedback will help build face validity. After this step, small changes and adjustments will be applied based on the

players' feedback to remove confusion and to ensure the creative questionnaire is understood correctly. This subsection's result is clearly defined in Analysis Section 5.5. This step is the most important in the testing plan because it ensures that every question in the game measures what this study wants to measure.

3.5.5 User Interface Test

The interface test aims to evaluate system components, like the interaction between these interfaces and the way to control how they work. The team members developed a checklist with the specified design rules and requirements that all interfaces must satisfy regarding the following aspects.

Table 2. User Interface Test Checklist

Type of test	Expected Result	Actual Result
Hyperlinks accessibility	Quick access	Quick navigation
Smooth flow of the website	Smooth	Smooth
Proper font, size, and color	Perfect	Perfect
Smoothness while presenting the game's pictures and videos	Smooth	Smooth

4. Conclusion and Future Work

Since the science of computer networks began, their use has increased and thus the need for it has increased in all areas of life until it has become a necessity. On the other hand, there are some risks that threaten institutions that rely on networks, especially when using the Internet. This study was introduced to measure human behavior via a creative questionnaire and to facilitate measuring behavior in terms of a specific pattern. This study identified the major problem with human behavior, which is that humans must be more conscious of the security policy to behave correctly. Moreover, this topic is illustrated and justified based on a review of the literature. It also justified the security measures needed for measuring human behavior regarding policies of cybersecurity. On the other hand, this study has problems and objectives that require several steps to be completely solved to reach the ideal solution. Creating an ideal and safe environment to measure the behavior and to analyze the whole study are this study's main objectives.

This study scope includes measuring human behavior toward cybersecurity policies. So, its scope is to establish an attractive method to help measure human behavior without any restrictions. The study reached the ideal method mentioned above, which is the creative questionnaire. This method is based on a specific pattern that introduces multiple stages, starting with measures selecting and ending with questionnaire's forming. The first stage chooses the measures that must be taken for measuring human behavior. Based on a review of the literature five measures were selected. These measures are important in terms of security policies. In the second stage, each measure has corresponding security policies that were reviewed and validated by the panel of experts as important policies about the measures. Third, all the questions related to each policy were displayed and included in the scenario. Fourth, these scenarios were transformed into action in the game.

References

[1] Herath, T. and H.R. Rao, (2009) *Encouraging* information *security behaviors in organizations: Role of penalties, pressures and perceived effectiveness.* Decision Support Systems. **47**(2): p. 154-165.

[2] Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? how do we get it? In "Security and Usability: Designing Secure Systems that People Can Use." Edited by L. Cranor and S. Garfinkel.

[3] Anwar, M., et al., (2017) Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior. 69: p. 437-443.

[4] Borges, P.V.K., N. Conci, and A. Cavallaro, (2013) Video-Based Human Behavior Understanding: A Survey. IEEE Transactions on Circuits and Systems for Video Technology. 23(11): p. 1993-2008.

[5] Alissa, K.A., et al. (2018) An Instrument to Measure Human Behavior Toward Cyber Security Policies. in 2018 21st Saudi Computer Society National Computer Conference (NCC).

[6] Voiskounsky, A.E., O.V. Mitina, and A.A. Avetisova, (2004) Playing online games: Flow experience. PsychNology journal. 2(3): p. 259-281.

[7] Okuneva, M. and D. Potapov, (2014) Consumer behavior in online games. Higher School of Economics Research Paper No. WP BRP. 25.

[8] Kou, Y., M. Johansson, and H. Verhagen, (2017) Prosocial behavior in an online game community: an ethnographic study, in Proceedings of the 12th International Conference on the Foundations of Digital Games2017, Association for Computing Machinery: Hyannis, Massachusetts. p. Article 15.

[9] Yang, R., et al. Game Theory and Human Behavior: Challenges in Security and Sustainability. (2011). *In International Conference on Algorithmic DecisionTheory* pp. 320-330. Springer, Berlin, Heidelberg.

[10] Rees, J., S. Bandyopadhyay, and E.H. Spafford, (2003) PFIRES: a policy framework for information security. Communications of the ACM. 46(7): p. 101-106.

[11] Stoneburner, G., A. Goguen, and A. Feringa, (2002) Risk management guide for information technology systems. Nist special publication. 800(30): p. 800-30.

[12] Stanton, J.M., et al. (2005) Analysis of end user security behaviors. Computers & Security. 24(2): p. 124-133.

[13] Ng, B.-Y., A. Kankanhalli, and Y. Xu. (2009) Studying users' computer security behavior: A health belief perspective. Decision Support Systems. 46(4): p. 815-825.

[14] Ross, R., et al. (2015) Recommended security controls for federal information systems. NIST Special Publication. 800: p. 53.

[15] Pahnila, S., M. Siponen, and A. Mahmood. (2007) Employees' Behavior towards IS Security Policy Compliance. in 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07).

[16] Evans, M., et al. (2016) Human behaviour as an aspect of cybersecurity assurance. Security and Communication Networks. 9(17): p. 4667-4679.

[17] Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of Cybersecurity Standard and Framework Components. International Journal of Communication Networks and Information Security, 12(3): p.417-432.

[18] M. M. Umer, S. Khan, R. Ahmed, D. Singh, Game Theoretic Reward Based Adaptive Data Communication in Wireless Sensor Networks, IEEE ACCESS Journal, Vol. 6, pp.28073-28084, 2018.

[19] K. Khan, A Mehmood, S. Khan, A. Khan, Z. Iqbal, A survey on intrusion detection and prevention in wireless ad-hoc networks, Journal of Systems Architecture, Vol. 105, May 2020.