# AHP-based Security Decision Making: How Intention and Intrinsic Motivation Affect Policy Compliance

Ahmed Alzahrani[1], Christopher Johnson[2]
School of Computing Science
University of Glasgow
Glasgow, UK

***Abstract*—Analytic hierarchy process is a multiple-criteria tool used in applications related to decision-making. In this paper, analytic hierarchy process is used as guidance in information security policy decision-making by identifying influencing factors and their weights for information security policy compliance. The weights for intrinsic motivators are identified based on self-determination theory as essential criteria, namely, autonomy, competence, relatedness, along with behavioural intention towards compliance; and use four awareness focus areas. A survey of cyber-security decision-makers at a Fortune 600 organisation provided data. The results suggest that behavioural intention (52% of the weight of influencing factors) is more important than autonomy (21%), competence (21%) or relatedness (6%) in influencing behaviour towards information security policy compliance. Determining weights of intrinsic motivation, intention, and awareness focus areas can help security decision-making and compliance with policy, and support design of effective security awareness programmes. However, these weights may in turn be affected by local organisational and cultural factors.**

***Keywords—Analytic Hierarchy Process; behavioural intention; autonomy; competence; relatedness; information security policy compliance***

## I. Introduction

Policy decision making is one of the most challenging tasks in the field of information security and compliance. It must consider multiple aspects in a stable form to for appropriate decision making to deal with the actual situation as well as future planning.

Analytic Hierarchy Process (AHP), initially developed by Thomas L. Saaty in 1972 [1], is widely used in the Multi-Criteria decision-making method to solve complex decision problems. AHP quantifies related priorities for specific alternatives on a scale according to decision-makers' judgment [2]. It uses both mathematics and the psychology of human decision-making based on pair-wise comparisons to measure the criteria for a specific problem [3]. Moreover, it helps regulate tangible and intangible criteria in an organised way by providing a simple solution to the decision-making problem. It also provides a comparison of both quantitative and qualitative information based on decision-makers' judgements to obtain weights and priorities [2]. The AHP approach uses hierarchical levels for decomposing a complex problem into multiple sub-problems. The first level represents the goal of decision making, and the higher levels represent a set of criteria and alternatives [4] (see Section III, Fig. 2).

In this paper, the three essential elements of self-determination theory (SDT), autonomy, competence and relatedness have been extensively used. They were analysed for their potential to enhance the intrinsic motivation of employees and, their behavioural intention toward security policy compliance. SDT, developed by Deci and Ryan [5] helps to understand developmental and psychological requirements for analysing the roots of motivation and personality. This theory focuses on an individual's behaviour, self-motivation and determined for target behaviour. Motivation is divided into extrinsic and intrinsic motivation, along with the three psychological requirements of competence, autonomy and relatedness [5][6]. SDT has been chosen for two reasons: From a theoretical perspective, adoption of SDT in the field of information security is under-researched, even though SDT has successfully improved intrinsic motivation in fields like health and education. From a practical standpoint, the results of this study can help provide an organisation with a new perspective on the ability of intrinsic motivation to encourage compliance and, ultimately, address a wide range of potential security vulnerabilities.

Further, the AHP method for guiding policy decision-making was used to determine the factors and their weights for ensuring compliance with ISPs. This analysis indicates that determining weights of intrinsic motivation factors, and awareness focus areas, can potentially help decision-making on security compliance policy and designing proper security awareness programmes for an organisation, as discussed in Section 6.

This paper examines AHP as a method to support cyber security decision-making within a Fortune 600 organisation. The paper uses AHP to identify the weights for intrinsic motivation and behavioural intention to comply with the information security policy, which helps security decision-makers design suitable security awareness programmes.

The paper is organised as follows: Section II provides a review of related work in the field. Section III describes the methodology followed in conducting this study. Section IV presents the study analysis. The reporting results are presented and discussed in Section V, followed by recommendation in Section VI. Section VII presents the study limitations, avenues for future work and Section VIII presents the study conclusions.

## II. Background

### A. Theoretical Foundation

Information security policy is a challenging field for decision makers, who face many dynamic aspects related to evolving cyber-security threats. Employee motivation plays an essential role in compliance with policy. An information security policy presents the acceptable practice of employees of an organisation and prescribes penalties for violations. There must be efforts to encourage employees toward compliance with the existing policy. This implies that the intrinsic motivation of employee to comply with information security policies can help to achieve long term advantages for the organisation. The significant factors involved in intrinsic motivation, in the SDT model, include autonomy, competence and relatedness, as described below.

*1) SDT component:* Autonomy refers to the desire of people to be able to choose a course of action that matches their inner beliefs [7]. It targets a personal desire for protecting their scope for action and decision-making [8]. A sense of autonomy supports an increase in intrinsic motivation to follow an organisation's rules, regulations and policies. Wall, Palvia, and Lowry [9] analysed the effect of autonomy as control-related motivation and the efficacy of employees' intentions toward policy compliance. The authors reported that an increased perception of autonomy increased the perception of efficacy, which improved employees' compliance with their organisations' policies.

Competence refers to the people's assessment of their ability to do the task at hand and their likelihood of obtaining the desired results [10]. It measures employees' perception of whether they have relevant skills to accomplish specific security tasks for compliance of information security policy. A sense of competence helps people feel confident in their ability to defend sensitive information of the organisation. Per SDT, competence is similar to self-efficacy for individuals' skills and abilities for performing a specific security task [11]. Thus, competence helps to reduce the stress and anxiety that are often related to information security policies like encryption and access control measures.

Relatedness measures an individual's requirement for remaining connected to others and being understood, valued and accepted by them. In SDT, relatedness is directly affected by the security culture within an organisation. Security culture involves employees' shared beliefs and values about cyber-security [12]. An increase in relatedness helps to increase the level of intrinsic motivation for compliance with information security policies. Organisational culture establishes the shared set of expectations and beliefs among members of the organisation, and partially determines the behaviour of each member of the organisation. Compliance is positively affected by a shared and accepted security culture [12].

*2) Behavioural intention:* Behavioural intention is a combined product of subjective norms, attitudes toward the behaviour, and perceived behavioural control [13]. A favourable opinion of a person towards behaviour and subjective norms leads to more perceived behavioural control and a firmer intention of the person to perform the target behaviour. In addition, individuals are supposed to present their intentions for providing chances for a given level of actual control over the behaviour [13]. The theory of planned behaviour focuses the knowledge for required skills in performing the behaviour, experience with the behaviour, and environmental factors [14]. The behaviour intention is determined by perceived behaviour control along with attitude and subjective norms. The jointly-established intention can be directly interpreted as the amount of control over the behaviour. The combined determination of the behaviour and the intention is related to motivation and a sense of control over the behaviour and hence affects compliance with information security policy.

### B. Analytic Hierarchy Process

Analytic hierarchy process (AHP) is widely used as a multiple-criteria decision-making tool for applications in diverse fields such as planning, selecting the best alternative, resource allocation, resolving conflicts, and optimisation. AHP is an appropriate tool for this study as it addresses the hierarchical requirements of the proposed model.

The AHP method has been widely used in banking, manufacturing systems, education, healthcare, the military, information technology and many other areas for more than thirty years [15], [16]. AHP supports planning, resource allocation, evaluation, development and optimisation [2], The study by Vaida and Kumar [16] provides a complete literary review.

In the context of information security, several studies have used AHP to evaluate information security policy from decision-making perspectives and for assessing information security awareness training.

Syamsuddin and Hwang [2], used the AHP approach to develop a framework for decision-makers to evaluate information security policy performance. To get decision-maker preferences, they used a survey based on AHP methodology prior to more detailed data analysis. The authors found that the availability of information security got the highest priority by decision makers, followed by confidentiality and integrity. Likewise, the authors used AHP to develop a model for information security policy decision making [17]. They used four security policy factors (management, technology, economy and culture) and three security components (confidentiality, integrity and availability) to develop their model. Their findings indicated that AHP helps policymakers make appropriate decisions by using qualitative and quantitative methods.

Syamsuddin [18] also evaluated information security policy decision-making in e-government systems via the AHP method. The results showed that decision-makers preferred management and technology as the essential aspects of information security and that availability of information was more important than other information security aspects. Also, the author stated that using AHP supported evaluation of the performance of information security policy in both qualitative and quantitative ways.

Kruger and Kearney [19] developed a prototype model for information security awareness measurement at an international gold mining company. The authors used AHP to determine the relative weights of information security awareness assessment across three dimensions (knowledge, attitude and behaviour). Also, their awareness programme used six focus areas (adhere to policies, keep password secret, email and internet, mobile equipment, incident reports and all actions carry consequences). A spreadsheet application was used to process importance weights based on the AHP method. In their findings, they stated that the effectiveness of measurement by the model relies on the importance weightings that must be obtained from key management's professional judgement.

Kruger and Kearney [20] used AHP to determine the relative importance weights for knowledge, attitude and behaviour to implement an information-security awareness programme. They used AHP to determine the weights of alternative elements (the awareness programme topics were: adhere to policies, keep password secret, email and internet, mobile equipment, incident reports, and all actions carry consequences) in the AHP model. According to key managers' professional judgements and opinions, behaviour had an importance weight of 50% compared to knowledge (30%) and attitude (20%). Whereas the main security principles (confidentiality, integrity and availability) focus on protecting information, security awareness helps the organisation create and sustain the positive security behaviour of employees [19]. Hence, the organisation will ensure that employees do not create expensive, avoidable mistakes concerning information security and that they will have a good understanding of their information security policy and procedures [21][22].

## III. Methodology

The flowchart of the proposed method is shown in Fig. 1. Further details are in the following sections.

### A. Study Method Assessment and Refinement of Measurement Scales

Two independent researchers in the AHP field confirmed the study method. They also conducted a final validation of the AHP questionnaire before it was distributed. Their feedback helped to improve the questionnaire's design.

### B. Data Collection Procedure

The AHP questionnaire was shared with a Fortune 600 organisation to obtain responses from cyber-security managers and experts. The head of the information security awareness group was asked to send an email including the survey link and a description of the study objectives to security managers and experts. The participants were not asked to state their names or email addresses. As shown in Table I, an AHP preference scale [23] was used for this study to derive priorities for each factor in the form of questions such as, "How important is autonomy compared to competence?" (cf. Appendix1, Section A.1).

### C. The Proposed Decision Model

To determine the important weights for autonomy, competence, relatedness, and intention, a new model is proposed as seen in Fig. 2. The model is divided into a three-level hierarchy based on the previous literature study. Level one shows the goal of this study, which is information security weight decision making, followed by three components of SDT with intention in level two and four security awareness focus areas in the third level. The security awareness focus areas were selected based on the incidents report from a Fortune 600 organisation and was validated by security managers and experts within the same organisation.

### D. AHP Method

The AHP method can easily be applied to a complex decision problem in four steps [24], as given in the instructions below.

- Step 1: Define the decision problem as a hierarchy. This is the most important aspect of AHP; the problem is decomposed into a hierarchy of like elements as shown in Fig. 2. The model includes three levels (goal, criteria and alternatives).

- Step 2: Use pairwise comparisons of decision elements. Break down the problem into a hierarchy to obtain the local weight of each element. This step compares an element of a specific level in relation to an element in the level directly above it.

- Step 3: Calculate the local weights and consistency of comparison matrices. The local weights of all elements are determined using the eigenvalue method (EVM). "The normalised eigenvector corresponding to the principal eigenvalue of the judgement matrix provides the weights of the corresponding elements" [2].

- Step 4: Obtain the final weights of elements by aggregating the weights of decision elements across different levels. Here, the local weights of decision elements from all levels are aggregated to calculate the final weights of the alternatives (security awareness focus areas in the third level).

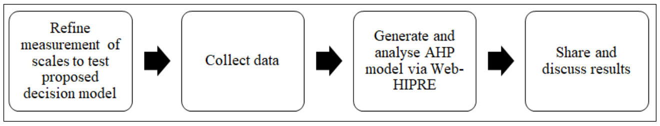

Refine measurement of scales to test proposed decision model
Collect data
Generate and analyse AHP model via Web-HIPRE
Share and discuss results

Fig. 1. Flowchart of the Proposed Method.

TABLE I. Saaty's Pairwise Comparison Scale

| Scale value | Definition Criterion X in comparison to Y |
|---|---|
| Equal Importance | 1 |
| Equally to Moderately | 2 |
| Moderate Importance | 3 |
| Moderately to Strong | 4 |
| Strong Importance | 5 |
| Strongly to very strong | 6 |
| Very strong Importance | 7 |
| Very strong to extremely | 8 |
| Extreme Importance | 9 |

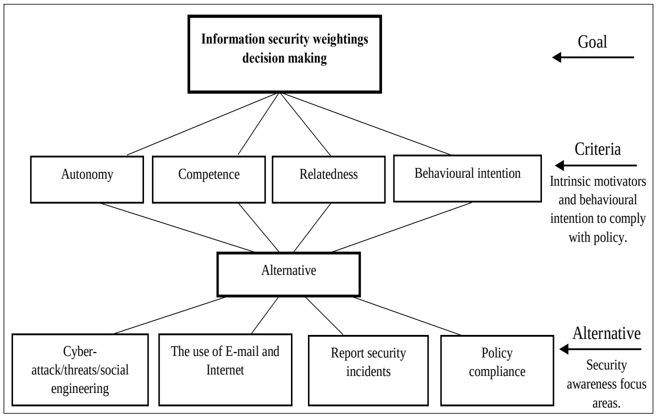

Information security weightings decision making
Goal
Autonomy
Competence
Relatedness
Behavioural intention
Criteria
Intrinsic motivators and behavioural intention to comply with policy.
Alternative
Cyber-attack/threats/social engineering
The use of E-mail and Internet
Report security incidents
Policy compliance
Alternative
Security awareness focus areas.

Fig. 2. Information Security Weighting Decision-Making Model.

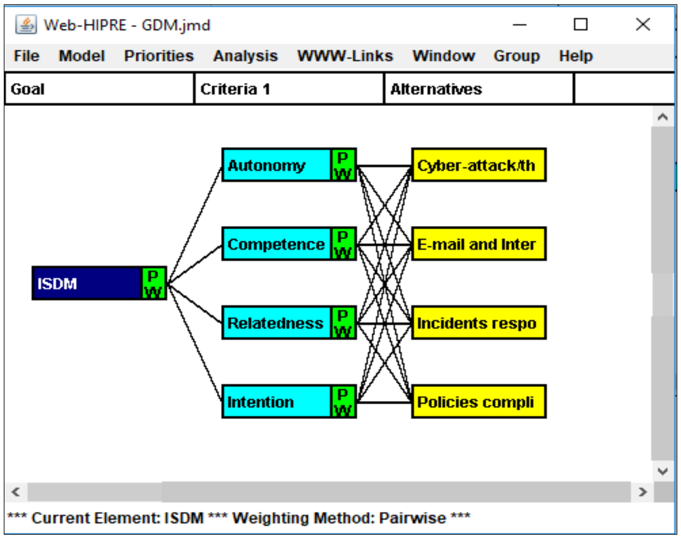
## IV. Data Analysis

This study makes use of the Web-HIPRE to generate and analyse the AHP model. Web-HIPRE is an adaptation of AHP which enables a decision maker to form a robust decision model [25]. The complex decision problem is entered by providing general labels in the decision tree, at each of the node levels. After that, the problem components need to be entered. Then, to make effective use of the Web-HIPRE algorithms, the user must enter pair-wise preferences at every node level for criteria, sub-criteria and alternatives. After this process has been carried out, the suitable analysis algorithm is used to determine the model's recommendation. The algorithm of Web-HIPRE makes it possible to perform sensitivity analysis. This process ascertains the criteria or sub criteria which play a dominant role in the entire decision-making process. The algorithm is designed so it can be employed to a group mode as well. The algorithm of WebHIPRE allows an issue or problem to be structured based on specific criteria and alternatives. Then each of the critical decision-making components is linked with web pages so that the specific details relating to the criteria, sub-criteria and alternatives can be understood in a simpler manner. The Web-HIPRE software uses AHP to calculate the consistency measure (CM) using the formula shown in Fig. 3.

In this formula, "r(i,j)=max a(i,k)a(k,j), k ∈ {1,..,n} stands for the extended bound of the comparison matrix element a(i,j), and r(i,j) is the inverse of r(j,i).Thus, the consistency measure is an indicator of the size of this extended region formed by the set of local preferences such that Wi ≤ r (i,j)Wj for all i,j ∈ {1,..,n}" [25]. For example, as shown in (Appendix 1, Section A.1: criteria comparisons), participating security decision-makers were asked to respond to pairwise comparison questions of autonomy, such as, "How important is the cyber-attack awareness focus area relative to the use of internet and email awareness focus area?" The decision-makers could use local organisational and cultural factors to choose the proper awareness focus area that would best address autonomy motivator needs. After that, Web-HIPRE was used to find the CM of the pairwise comparison of autonomy according to the decision-makers' inputs. As shown in Table 3, the cyber-attack awareness focus area had the top priority consideration of 0.568, with a CM at an acceptable level of 0.060, which is less than Saaty's maximum acceptable value of 0.10 [23].

$$CM = \frac{2}{n(n-1)} \sum_{i>j} \frac{\bar{r}(i,j) - \underline{r}(i,j)}{(1+\bar{r}(i,j))(1+\underline{r}(i,j))}$$

Fig. 3. Consistency Measure Formula.



*** Current Element: ISDM *** Weighting Method: Pairwise ***

Fig. 4. Information Security Decision Making (ISDM) Model.

CM is a vital element of Web-HIPRE as it converts inconsistent decision elements or replies into an "extended" series of appropriate preference statements. It helps to mitigate the inconsistencies that could arise in the decision-making process and makes it more uniform in nature. The measure basically ranges between 0 and 1, and its value gets higher with an increase in the inconsistency of the comparison matrix elements. The algorithm establishes interconnections among the core decision-making elements. This helps to arrive at the final decision that can be implemented to solve the problem at hand. One of the unique aspects of the algorithm is the ability to structure the entire issue in smaller segments so that each of the core decision-making components can be critically considered by the software.

Fig. 4 shows the first step of the AHP analysis method, which defines the decision problem as a hierarchy. The figure shows the AHP model developed in Web-HIPRE, based on Fig. 2 that includes four criteria and four alternatives to achieve the study goal. Subsequently, all responses from respondents are inserted into the compression windows for each intrinsic motivator, as well as for intention to comply with ISP.

## V. Results and Discussion

Tables II to VII show the complete paired comparison matrix. Respondents' inputs were used to make a pairwise comparison for each factor depicted in 3. Table II illustrates the pairwise comparison of criteria with respect to the goal, based on the second step of the AHP analysis method. It is clearly showed that intention is the most important factor among the three components of SDT and controls 57% of overall information security weighted decision making. Autonomy and competence factors controlled similar importance weights of

18.7% and 17.5% respectively. The relatedness factor had the lowest priority among all other factors, with 6.7% of local weight. As can be seen in Table II, the consistency ratio value is 0.081, which means good consistency since it's below Saaty's maximum acceptable value of 0.10 [23].

Tables III to VI explain the local weights of comparative alternatives based on four criteria that define the local weight value of the four security awareness focus areas (cyber-attack, the use of email and internet, incident response and policy compliance) according to the third step of the AHP analysis method. Respondents' inputs were used to make a pairwise comparison for each factor, as shown in (Appendix 1, Section A.2 to A.5). The consistency measure values of these factors are below the acceptable value of 0.10, showing very good consistency. To get the overall priorities of all decision factors, all factors' local weights were calculated and aggregated them into an overall weight value as shown in Table VI. Policy compliance is preferred as the top awareness focus area with the value of 0.293, followed by use of email and internet and incident response, which have similar priority values of 0.255 and 0.259. Cyber-attack accounted for only 0.193. The final result indicated that intention, with 52%, is considered more important than the other three components of SDT. Autonomy and competence have similar importance priorities of approximately 21%. Relatedness accounted for 6%.

According to these findings, decision-makers in the organisation put the most emphasis on policy compliance as the top priority among all other alternatives or awareness focus areas (the others being cyber-attack, the use of email and internet and incident response). This also reflects the top priority of intention towards compliance in the organisation among the other three components of SDT. Hence, decision-makers believe that employees' intentions play an essential role in policy compliance in the organisation, along with autonomy and competence. On the other hand, decision-makers considered relatedness as the lowest priority among all elements, and that it had a minimal effect on employee behaviour towards policy compliance.

TABLE II. PAIRWISE COMPARISON OF CRITERIA

| | **Autonomy** | **Competence** | **Relatedness** | **Intention** | **Local weight** |
|---|---|---|---|---|---|
| Autonomy | 1.0 | 1.0 | 3.0 | 0.33 | 0.187 |
| Competence | 1.0 | 1.0 | 3.0 | 0.25 | 0.175 |
| Relatedness | 0.33 | 0.33 | 1.0 | 0.14 | 0.067 |
| Intention | 3.0 | 4.0 | 7.0 | 1.0 | 0.571 |
| Consistency Measure = 0.081 | | | | | |

TABLE III. PAIRWISE COMPARISON OF AUTONOMY

| | **Cyber-attack** | **E-mail and Internet** | **Incidents response** | **Policies compliance** | **Local weight** |
|---|---|---|---|---|---|
| Cyber-attack | 1.0 | 4.19 | 4.22 | 3.52 | 0.568 |
| E-mail and Internet | 0.24 | 1.0 | 1.0 | 1.17 | 0.148 |
| Incidents response | 0.24 | 1.0 | 1.0 | 0.85 | 0.136 |
| Policies compliance | 0.28 | 0.85 | 1.17 | 1.0 | 0.148 |
| Consistency Measure = 0.060 | | | | | |

TABLE IV. PAIRWISE COMPARISON OF COMPETENCE

| | **Cyber-attack** | **E-mail and Internet** | **Incidents response** | **Policies compliance** | **Local weight** |
|---|---|---|---|---|---|
| Cyber-attack | 1.0 | 0.3 | 0.3 | 0.25 | 0.086 |
| E-mail and Internet | 3.29 | 1.0 | 1.04 | 0.83 | 0.288 |
| Incidents response | 3.38 | 0.96 | 1.0 | 1.13 | 0.308 |
| Policies compliance | 3.99 | 1.2 | 0.88 | 1.0 | 0.319 |
| Consistency Measure = 0.063 | | | | | |

TABLE V. PAIRWISE COMPARISON OF RELATEDNESS

| | **Cyber-attack** | **E-mail and Internet** | **Incidents response** | **Policies compliance** | **Local weight** |
|---|---|---|---|---|---|
| Cyber-attack | 1.0 | 0.3 | 0.32 | 0.29 | 0.093 |
| E-mail and Internet | 3.28 | 1.0 | 1.0 | 1.0 | 0.303 |
| Incidents response | 3.09 | 1.0 | 1.0 | 0.91 | 0.291 |
| Policies compliance | 3.4 | 1.0 | 1.1 | 1.0 | 0.313 |
| Consistency Measure = 0.018 | | | | | |

TABLE VI. PAIRWISE COMPARISON OF INTENTION

| | Cyber-attack | E-mail and Internet | Incidents response | Policies compliance | Local weight |
|---|---|---|---|---|---|
| Cyber-attack | 1.0 | 0.34 | 0.39 | 0.3 | 0.102 |
| E-mail and Internet | 2.94 | 1.0 | 0.83 | 0.97 | 0.284 |
| Incidents response | 2.59 | 1.2 | 1.0 | 0.84 | 0.291 |
| Policies compliance | 3.31 | 1.03 | 1.19 | 1.0 | 0.324 |
| Consistency Measure = 0.069 | | | | | |

TABLE VII. FINAL RESULT

| Goal | Cyber-attack | E-mail and Internet | Incidents response | Policies compliance | Overall weight |
|---|---|---|---|---|---|
| Autonomy | 0.119 | 0.031 | 0.028 | 0.031 | 0.209 |
| Competence | 0.018 | 0.060 | 0.064 | 0.066 | 0.207 |
| Relatedness | 0.006 | 0.019 | 0.018 | 0.020 | 0.063 |
| Intention | 0.051 | 0.145 | 0.148 | 0.176 | 0.521 |
| Overall weight | 0.193 | 0.255 | 0.259 | 0.293 | |

## VI. RECOMMENDATION

The AHP results can be used to design a proper security awareness programme which may help to enhance policy compliance. Also, this results can be used for data processing and transform it into meaningful information using the matrices presented in Table VII such as [19][20]. As shown by the final results in Table VII, the following are recommended when designing an awareness programme based on intrinsic motivation on the basis of SDT:

### A. Autonomy

As shown in Table VII, cyber-attack has the highest priority value of 0.119 over other awareness focus areas toward autonomy. Since autonomy focuses on the desire to protect an individual's scope for action and decision-making [8], [20], it is recommended that the organisation develop suitable awareness programmes that focus on cyber-attacks, threats and social engineering to increase employees' decision-making ability when they face real-world attacks.

### B. Competence

As can be seen in Table VII, the awareness focus areas related to competence (use of email and internet, incident response and policy compliance) have similar priority values of 0.060, 0.064 and 0.066 while cyber-attack has only 0.018. As a result, since competence measures employees' perception of whether they possess the relevant skills to achieve particular security tasks, it is recommended that the organisation focus on those three areas to increase employees' security knowledge.

### C. Relatedness

While it has the lowest priority value among the other factors, it is still recommended that the organisation develop suitable awareness programmes that focus on the use of email and internet, incident response and policy compliance, because they have similar priority values of 0.019, 0.018 and 0.020. Cyber-attack has only 0.006. The awareness programme should meet the relatedness requirements: the individual's need to be understood, valued, accepted, and connected to others. This would be achieved either in class or online awareness courses to encourage involvement, participation, and discussion among employees. If they share good security knowledge with each other, employees will be more likely to comply with their organisation's security policy.

### D. Intention

As shown in Table VII, the awareness focus areas related to intention (use of email and internet, incident response and policy compliance) have a similar priority value of 0.145, 0.148 and 0.176, while cyber-attack has only 0.051. Intention has the highest priority among the factors and it refers to activities employees must carry out to maintain information security as defined by their organisation's policy. Therefore, it is recommended that the organisation develop awareness programmes that focus on these areas to increase employees' intentions towards compliance. Employees who show less than suitable behaviour with regard to their organisation's policy might benefit from regular awareness sessions and training. The primary goals of security awareness are to enhance employees' behaviour towards policy compliance and to establish good security practices.

## VII. LIMITATIONS AND FUTURE WORK

Despite efforts to increase accuracy, this study has a notable limitation: it only used data collected from cyber-security managers and experts of a single large organisation in Saudi Arabia, which potentially undermines its generalisability. Future research may consider conducting the study with a different organisation or even in another country to explore the generalisability of its results and provide more evaluation of the information security weighing decision-making model.

This study demonstrates that AHP is powerful method to support decision-making about complex sustainability issues. Also, AHP helped participating decision makers recognise and outline complex problem in detail. However, despite the strengths of AHP, there are some issues with its methodology. Since AHP can divide a complex problem into a number of sub-levels, this may lead to very large number of pairwise comparisons that must be made. Processing the input for each sublevel can be time-consuming. Decision-makers who took part in this study had difficulty using the 9–point scale (see Table I). They reported that it was difficult to distinguish between the nine points to decide, for example, whether one criteria or alternative was 6 or 7 times more important than another. The scale problem seems to be common and some researchers, such as Hajkowicz *et al.* [26] modified the procedure by using a 2‒point scale, (more or less important or equally important) in the field of natural resources management. Hence, future work of this study may conduct more research into the applicability of an alternative to the 9‒point scale in the field of security policy compliance. This may help participants provide their feedback with fewer restrictions and less confusion.

## VIII. Conclusion

In conclusion, this study attempts to help organisations determine the important factors and their weights for information security decision making by using the AHP method. Using AHP, this study proposes a model that uses four criteria (autonomy, competence, relatedness, and intention) and four alternative awareness focus areas (cyber-attack, the use of email and internet, incident response and policy compliance). The study demonstrates that intention represents the highest priority, followed by autonomy and competence while relatedness has the lowest weight. Also, the study concludes that policy compliance, the use of email and internet and incident response are the essential security awareness topics that should be addressed under the requirements of competence, relatedness, and intention. In contrast, the result recommends using only cyber-attack, threats and social engineering awareness topics to discuss the needs of autonomy to increase employees' decision-making ability when they face real-world attacks.

## References

[1] T. L. Saaty, "An eigenvalue allocation model for prioritization and planning," Energy Manag. Policy Center, Univ. Pennsylvania, pp. 28–31, 1972.

[2] I. Syamsuddin, J. H.- JSW, and undefined 2010, "The Use of AHP in Security Policy Decision Making: An Open Office Calc Application.," Citeseer.

[3] T. S.-I. journal of services sciences and undefined 2008, "Decision making with the analytic hierarchy process," inderscienceonline.com.

[4] A. Fakouri, H. Pasha, P. Jalili, and S. Abdollahzadeh, "Ranking the captech technology strategies by integrating fuzzy ahp and fuzzy topsis methods."

[5] R. Ryan and E. Deci, "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being.," Am. Psychol., vol. 55, no. 1, pp. 68–78, 2000.

[6] R. M. Ryan and E. L. Deci, Self-determination theory: Basic psychological needs in motivation, development, and wellness. Guilford Publications, 2017.

[7] 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.

[8] 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, pp. 125–132.

[9] J. Adie, J. 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," Psychol. Sport Exerc., 2012.

[10] L. Vandercammen and J. Hofmans, "The mediating role of affect in the relationship between need satisfaction and autonomous motivation," J. Occup., 2014.

[11] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," Comput. Secur., vol. 31, no. 1, pp. 83–95, 2012.

[12] G. Greene and J. D'Arcy, "Assessing the impact of security culture and the employee-organization relationship on IS security compliance," Symp. Inf. Assur., 2010.

[13] I. Ajzen, "Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior 1," J. Appl. Soc. Psychol., vol. 32, no. 4, pp. 665–683, Apr. 2002.

[14] M. S. Hagger and N. L. D. Chatzisarantis, "Integrating the theory of planned behaviour and self-determination theory in health behaviour: A meta-analysis," Br. J. Health Psychol., vol. 14, no. 2, pp. 275–302, May 2009.

[15] A. Ishizaka, A. L.-E. systems with applications, and undefined 2011, "Review of the main developments in the analytic hierarchy process," Elsevier.

[16] O. Vaidya, S. K.-E. J. of operational research, and undefined 2006, "Analytic hierarchy process: An overview of applications," Elsevier.

[17] J. Hwang, I. S.-& Simulation, 2009. AMS'09. Third, and undefined 2009, "Information Security Policy Decision Making: An Analytic Hierarchy Process Approach," ieeexplore.ieee.org.

[18] I. Syamsuddin, J. H.-J. of Simulation, undefined Systems, S. and, and undefined 2009, "The application of AHP to evaluate information security policy decision making," ijssst.info.

[19] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," Comput. Secur., vol. 25, no. 4, pp. 289–296, Jun. 2006.

[20] H. Kruger and W. Kearney, "Measuring information security awareness: A West Africa gold mining environment case study," 2005.

[21] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: an action research study," Mis Q., pp. 757–778, 2010.

[22] C. Brodie, "The Importance of Security Awareness Training The Importance of Security Awareness Training The Importance of Security Awareness Training GIAC Gold Certification The Importance of Security Awareness Training."

[23] T. L. Saaty and J. M. Katz, "How to make a decision: The Analytic Hierarchy Process," Eur. J. Oper. Res., vol. 48, pp. 9–26, 1990.

[24] F. Z.- interfaces and undefined 1986, "The analytic hierarchy process—a survey of the method and its applications," pubsonline.informs.org.

[25] J. Mustajoki and R. P. Hämäläinen, "Web-Hipre: Global Decision Support By Value Tree And AHP Analysis," INFOR Inf. Syst. Oper. Res., vol. 38, no. 3, pp. 208–220, Aug. 2000.

[26] S. Hajkowicz, M. Young, D. H. MacDonald, and others, "Supporting decisions: Understanding natural resource management assessment techniques," 2000.

## Appendix 1

The following example explains a paired comparison for participants:

Suppose you have two mobile phone brands Apple and Samsung. Which mobile phone brand do you like better than the other and how much better do you like it in comparison with the other? Use this relative scale to measure how much you like the mobile phone brand on the left (Apple) compared to the mobile device on the right (Samsung).

If you like the Apple better than Samsung, mark between number 1 and 9 on the left side; if you favour Samsung more than Apple, mark on the right side.

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Apple | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Samsung |

## A. *Questionnaire*

For each section, the participants indicated how important factor A is relative to factor B by using the scale from 1- 9 as explained in Table I.

### *1)* Criteria comparisons.

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Autonomy | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Competence |
| Autonomy | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Relatedness |
| Autonomy | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Intention |
| Competence | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Relatedness |
| Competence | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Intention |
| Relatedness | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Intention |

### *2)* Pairwise comparisons of autonomy

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cyber-attack | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Use of e-mail and Internet |
| Cyber-attack | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Incidents response |
| Cyber-attack | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Policies compliance |
| Use of e-mail and Internet | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Incidents response |
| Use of e-mail and Internet | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Policies compliance |
| Incidents response | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Policies compliance |

### *3)* Pairwise comparisons of competence

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cyber-attack | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Use of e-mail and Internet |
| Cyber-attack | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Incidents response |
| Cyber-attack | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Policies compliance |
| Use of e-mail and Internet | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Incidents response |
| Use of e-mail and Internet | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Policies compliance |
| Incidents response | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Policies compliance |

### *4)* Pairwise comparisons of relatedness

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cyber-attack | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Use of e-mail and Internet |
| Cyber-attack | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Incidents response |
| Cyber-attack | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Policies compliance |
| Use of e-mail and Internet | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Incidents response |
| Use of e-mail and Internet | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Policies compliance |
| Incidents response | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Policies compliance |

### *5)* Pairwise comparisons of intention

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cyber-attack | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Use of e-mail and Internet |
| Cyber-attack | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Incidents response |
| Cyber-attack | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Policies compliance |
| Use of e-mail and Internet | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Incidents response |
| Use of e-mail and Internet | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Policies compliance |
| Incidents response | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Policies compliance |