A Framework to ensure Information Security Awareness in the Middle East

Fatima A Almarshad[1], Abdullah I A Alzahrani[2], and Gary Wills[1]

1 School of Electronics and Computer Science, University of Southampton 2 Department of Computer Science, Al Quwaiiyah, Shaqra University

Abstract
The reliance on information systems within business in all societies, brings about the need for trust and security in their use. Technology is considered to be the foundation for securing such systems. However, technology alone is not enough, since users make mistakes, both in unwittingly and intentionally, which is why there is a need for well-defined information security awareness policies and practices that reduce the risk of incidents through continual assurance. Culture has been found to play a significant role when implementing awareness strategies, since the impact of information security awareness programmes has varied in their impact, and is influenced by national culture. This paper defines the essential factors that have to be maintained in Middle-Eastern organisations in order to implement effective awareness strategies. In considering culture, we present a synthesis of features and components highlighted in the literature. This was supplemented by interviews with experts in information security about attitudes and behaviours among employees in their institutions. Current information security management systems standards were checked for security awareness in their policies. A framework of factors was created by applying thematic analysis to characterise information security awareness. The significant components of the framework were the factors that frame awareness in the light of cultural and environmental perspectives: Knowledge, Attitude, and Behaviour.

Keywords: *Awareness strategy, cultural impact, information security awareness, information security culture, user behaviour*

1. Introduction

Despite advances in technologies and techniques in information security, organisations are still witnessing intrusions. Many studies argue that users pose the main threat to protected information due to their frequent involvement in information operations (Aydın & Chouseinoglou, 2013; Bulgurcu, et al., 2010; Kweon, et al., 2021; McCormac, et al., 2017). Although information security specialists might be effective in implementing proactive measures and reducing the impact of security attacks, this is still insufficient to prevent harm or incursions from occurring. Users' deliberate or unintentional disregard of security policies and practices is the root cause of the problem. The implementation of information security awareness programmes has the potential to educate end-users as they are the key asset and the most vulnerable link. Many organisations use readily-available awareness programmes developed by international information security enterprises, while others create their own awareness tools according to the needs of their organisations. However, it has always been recognised that neither the one-size-fits-all programmes, nor the in-house programmes, have significantly influenced users' behaviour towards security risks.

This study explored the factors that influence the effectiveness of information security awareness strategies and programmes, and developed a framework that ensures an effective strategy for such awareness. The framework may help information security specialists design and implement an information security awareness programme that fits the culture, policies, and objectives of a given organisation, and ensure its effectiveness through countermeasures.

2. Background

Information security awareness has received remarkable attention in both industry and academia over the last two decades. The main concern is to ensure that all those within an organisation are aware of the rules and regulations regarding securing information systems that they manage. Previous studies have insisted that information security awareness should be an integral part of the overall information security strategy. Danchev (2003) concluded that ensuring information security in any organisation starts with an information security policy that defines what the user should and should not do, and ensure accurate and continuous monitoring of threats coming through the Internet that can infect the organisation's information system. It has also been pointed out that the level of knowledge and awareness of individuals in the organisation could influence the organisation's security plan, and that, to be effective, its plan must include improving those factors (Danchev, 2003). Research claims that the majority of people believe that most security threats come from hackers outside the organisation, so many institutions spend large sums to protect their information system from external threats (Bruck, 2002).

Bruck (2002) showed that 80% of attacks and threats came from within the organisation, from ex-employees having resentment against the organisation, and from

Manuscript received January 5, 2022
Manuscript revised January 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.1.76

employees who had been expelled from the organisation because they knew the vulnerabilities of the organisation's information systems. The last of these had the ability to gain unauthorised access to the organisation's systems, and thus were able to destroy or disable some sensitive areas of the systems. Protection of the information system lies in a combination of the development of security policy, effective policies to check and ensure the awareness level of the individual users, the presence of powerful anti-virus software and firewalls to protect the system, and relying on staff with experience and professionalism in the field of information security (Kazemi, et al., 2012).

Kreicberga (2010) investigated the factors that influence the security behaviour of employees, and how they perceive security measures against internal threats, by document reviews and direct observations of users' behaviour. He concluded:

- Employees comply with formal security requirements only if there are regular awareness methods
- Employee security behaviour is influenced by employer and colleagues' attitudes
- Strict technological countermeasures could hinder employee satisfaction and therefore motivates their negative behaviour
- Preservation and acceptance by staff of security measures is linked with their understanding of their benefits when implemented

The study recommended that continual assessments should be conducted of staff behaviour towards different security issues. In addition to keeping staff informed about the benefits that are achieved by their obligations to the measures to counter the threats faced by the institution's information systems, one popular way for fostering security culture and awareness in Saudi Arabia is compliance with information security management systems (ISMS) frameworks and standards, such as ISO27001, COBIT series, and HIPAA security framework for medical institutions. However, studies have reported that adoption does not sufficiently reflect the level of workforce awareness of information security risks and policies. This is due to weak support from senior management, ambiguity in understanding the standards' clauses, employee resistance to compliance policies, and poor development of effective awareness programmes by security teams (AbuSaad, et al., 2011). Although these standards touch on human components such as awareness and training, they do not focus on the employee or on how to direct, measure, and change their behaviour. This is supported by Sewuster (2013), who found that, while the security standard ISO27002 guidelines had been applied by security professionals belonging to local or regional government domains, employees of these organisations did not know the security risk assessments for the assets under their responsibility, regardless of their years of experience.

Employees' knowledge of information security risks, and their awareness of the preventive measures from attacks, are key factors that are important in securing an organisation's information. Every organisation must start with a security policy that provides all information about their security plan, which must then be followed by every employee, so the workflow is never interrupted by security issues and incidents. Awareness of the security policy, potential risks, and individuals' responsibilities are crucial factors that demonstrate the level of Information Security within an organisation that should be maintained, and which must be monitored frequently. This paper proposes a culture-based security framework for assuring information security awareness for Middle-Eastern organisations (FAISA).

3. The Framework Design and Methodology

This study is one phase of a large mixed methods project aimed at applying information assurance strategies in organisations. In this phase, the approach of Design Science (Hevner, et al., 2004) has been adopted in developing a localised, culturally sensitive and applicable Awareness framework (FAISA). Design Science enables unsolved serious problems to be researched in innovative and effective ways in the form of constructs, models, methods, instantiations, and better theories. The problem was formulated from the published literature, ISMS and international industrial standards, and semi-structured interviews with experts in relevant fields. These were the primary source of up-to-date information for describing the current state of Information Security culture problems and awareness challenges faced by organisations in Middle east.

TABLE 1: Qualifications of the Experts Interviewed

Expert	Job Domain	Area	Years of experience	Certificate
A	private	information assurance	18	+CISSP
B	government	information security	7	academic
C	government	information systems	24	+CISSP
D	government	information security	5	+ISO27001
E	private	health information management	14	academic
F	government	health information management	25	+CISSP
G	government	information security	5	academic
H	private	information assurance	13	+COPIT
I	government	information security	9	academic
J	government	information security	11	academic
K	government	information security	25	academic
L	government	information security	8	academic

The interviews, with both open and closed questions, were held with twelve experts, from different countries in the Middle-East. They verified the proposed factors and identified additional ones. Table 1 shows their qualifications. In the theory building stage, data were analysed and critical FAISA factors were identified and presented in a new framework as demonstrated in Figure 1. The new FAISA was reviewed and confirmed by the practitioners to further assure the newly-developed framework.

3.1 Approaches to Information Security Awareness Importance

Most research on information security awareness has resulted in calls for strengthening its importance within the work environment and fostering awareness initiatives. Techniques and guidelines have been provided on mechanisms and how to use them that are not necessarily based on a specific framework or model. Sommers & Robinson (2004) suggested that the use of awareness videos and quizzes can be used to train students at universities. However, there was no measure of the effectiveness of these methods, other than the theoretical quizzes after seeing the videos. Security awareness campaigns have been increasingly promoted by arranging mass media-based campaigns on certain risks and how to minimise them, such as leaflets, films, posters, and direct mail. Some have suggested that practitioners can educate users through IS security training software and by making IS security features more user friendly (Furnell, 2006).

Current research projects on information security focus on the human element. These studies have developed different frameworks, based on the Theory of Planned Behaviour, to measure a favourable or unfavourable manner towards a particular object. For instance, concerning information security awareness, Puhakainen (2006) and Kruger & Kearney (2006) developed frameworks that measure cognition, affect, and behaviour along three equivalent dimensions called knowledge (what does a person know), attitude (how do they feel about the topic), and behaviour (what do they do).

General Deterrence Theory (GDT), which was originally a criminology theory, has been used as the basis of other research, such as insider computer crime (Cardinali, 1995), and information security policy obedience (Vroom & Von Solms, 2004; Siponen, et al., 2007). All are aimed at minimising the threat that user behaviour poses to the protection of information assets.

These theoretical developments have proven to be effective in defining the factors that enhance awareness and prevent system abuse. Nevertheless, one of the main limitations of such research is that it addresses the problem only from an organisational perspective, and does not consider the effect of the external environment, and cultural differences among users.

3.2 Industrial Information Security Management Frameworks

For the framework development to be consistent with national and regulatory requirements, those international standards and frameworks for ISMS widely accepted and in use were consulted concerning awareness clauses, including training and education matters. The fourth control clause of Requirement 8.2.2 of ISO 27002 and ISO/IEC 27014 states that employees of the organisation who are granted access to any information system must be aware of their responsibilities and be provided with adequate training. In addition, training and education programmes must be specifically implemented based on a design and means of delivery that fits the purpose such as: posters, leaflets, presentations, and security events (ISO/IEC 27002-2013, 2013; ISO/IEC 27014:2020).

HIPAA (2021) on the other hand, states that all members of the workforce must be trained on policies and procedures of the security and the protection of health information within the entity as necessary and appropriate for them to do their functions.

According to Article 39(1)(b) of the GDPR (2018), Data Protection Officers are responsible for assuring compliance with the GDPR and other data protection provisions for the protection of personal data through assigning accountabilities, raising awareness and staff training, in operation processes, and the related audits.

Clause PO7.4 Personnel Training of COBIT 5.1, urges organisations to Provide IT employees with the appropriate ongoing training to ensure their skills, competence, and knowledge in a level that achieves organisational goals (ISACA, 2021). Clause DS.7 Education and Train Users, discusses the need for an education and training management process that ensures effective and efficient use of Information Technology solutions and applications that satisfies business requirements and ensures user compliance to policies and procedures. It stated that education and training programmes should be instituted and communicated; Education and training processes are documented and standardised; Security awareness and ethics practices are monitored and analysed.

IASME is the Information Assurance Management Standard intended to provide small and medium enterprises (SME) with a continuous assessment, adjustment, and determination of the maturity level of the security and protection of business information. Organisations can use it to assure themselves and others. IASME standards are characteristically simple, quick in adoption and cost effective, relying on the key elements of the international standards and guidelines promoted by the EU (Booth, 2015). It assesses the effectiveness of a business by evaluating 13 domains (Figure 1). One of its main evaluation domains is to measure the organisation personnel, managing, educating, and training them in business security. IASME emphasises comprehensive measures that ensure all employees are suitable from a security viewpoint before employment. These measures include adequate training, awareness of current threats and responsibilities, and the ability to debrief and removing privileges on termination of employment (Booth, 2015).

The issues encountered from the above standards is that they are all too general and can be vague to interpret, especially for non-expert teams.

3.3 The FAISA Framework

This paper proposes the Framework for Assuring Information Security Awareness (FAISA) which aims to provide organisations in the Middle East with measures that enable them to assess how aware their employees are about information security. It will also allow them to understand how to establish an information security culture that would cultivate an acceptable level of security awareness and minimise risks posed by employee behaviour on the use of information assets.

The FAISA developed in this paper is a novel framework based on Kruger & Kearney Model (2006). It has been constructed by systematically considering culture differences in various fields of knowledge that affect employees' attitudes and behaviour, which are influenced by both institutional and environmental drivers. In order to build an assured framework for information security awareness specifically for Middle Eastern organisations, each of the three dimensions in the model – knowledge, attitude, and behaviour – was then studied in detail, and linked to more focused areas which were confirmed by 33 practitioners in the field.

This resulted in four pillars to be assured informed by the institutional culture and the external environment. They adhere to Information security awareness policy, Information security awareness mechanisms, awareness of information security incident management, and the impact of information security awareness on employees' attitudes and behaviours, see Figure 1.

The institutional culture: Individuals' attitudes, values and beliefs about information security are shaped by the prevailing culture within the organisation. This could include cultural leadership, risk communication techniques, peer performance, and training programmes.

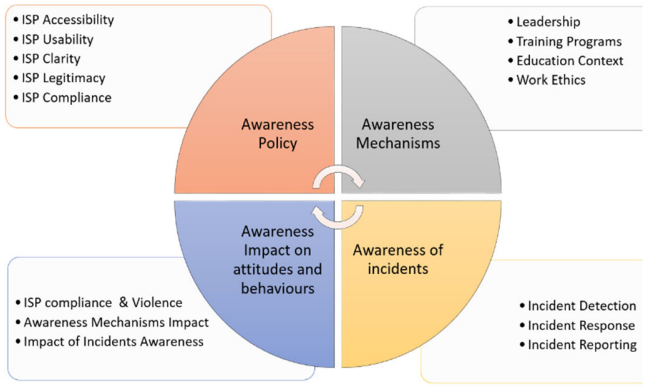


Figure 1: Information Security Culture Pillars

The external environment: This is an important factor that shapes individuals' attitudes and behaviour toward information security. Factors such as social pressure, created by individual tribes, friends and surrounding beliefs and religious indicators, have great influence on individuals' attitudes.

- **Information security policy**

The information security policy was in the top list of the awareness items in ISO 27001:2017. It has been defined as "a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point specific, covering a single area," SANS (2015). Experts have named three facts that should be considered in the development of the security policy: the huge cross-cultural differences in Middle-Eastern countries, users' lack of knowledge of the existence of the information security policy and its content, and users' unintentional violation of policy due the poor readability and understandability of the policy, or its usability.

Poor communication is seen as a cause of policy ignorance. Although there is information available for the users on the intranet, they do not actively seek knowledge of information security behaviour there. Proper communication might simplify user access to this documentation. It should ensure that knowledge is made explicit and disseminated to users.

In addition, it has been found that there are normally ambiguities around responsibilities. For instance, the organisation's staff must be aware of their personal responsibilities for information security assurance. Policy must be enacted through a strict hierarchy of responsibilities in order to assure information security policy has been met. Should a security incident arise, it is not clear who would ultimately be held to account, the member of the staff or their line manager. More importantly, to ensure that users accept the information security policy, it should not contradict their specific goals or hinder them from achieving them.

This is an important factor to be measured, which directly influences user behaviour toward policy compliance. This is done by considering usability factors and defining how to measure them, such as identifying possible risks, finding a balance with users' requirements, the scope of use, and measuring their effectiveness, efficiency, and user satisfaction.

Other ways to make people security conscious is through security education and training that emphasises removing vulnerabilities associated with human behaviour. Once the staff have a clear perception of the damage that the organisation might sustain in the event of an information security incident, their attitude should improve (Bauer, et al., 2017).

- **Awareness mechanisms**

It is important for education materials to be effective, and reflect the organisation's information security policies, and demonstrate the penalties for not following the rules.

Training techniques must provide motivation and knowledge of information security and all related practices. Such mechanisms as discussion meetings, problem solving and scenario thinking, should allow users to reflect on their personal information security situation. Education and training involve direct communication between information security

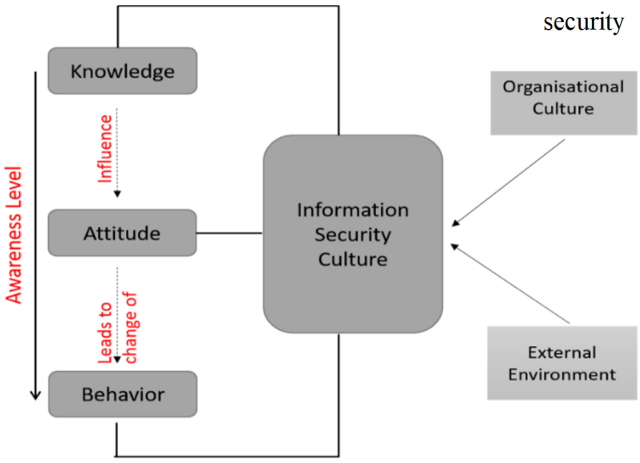


Figure 2: Assuring Information Security Awareness framework (FAISA)

professionals and users. Providing interactive learning, such as group meetings, can maintain social pressures of peer performance and tribalism. Culturally sensitive cybersecurity training and awareness programmes help close the communication gap and improve employee awareness and knowledge of cyber threats. Meanwhile, different cultures require different training and awareness, implying the need to design appropriate training and awareness programmes. This requires planning with clearly defined roles and responsibilities (for example, language and culture must be taken into consideration when preparing the awareness material).

Considering the strong direct influence of those with religious beliefs in that region, creating training and staff development programmes that enhance the quality of individuals through spiritual and religious values will lead to a positive effect on their information behaviour. Awareness training must inform personnel of information security risks associated with their activities, and their responsibilities in complying with the organisation's policies and procedures designed to reduce these risks. Interviewees also declared that training and education needs to be varied and given regularly to ensure sustainable long-term positive attitudes and behaviour.

- **Awareness of incident management**

A well-developed incident management policy cannot be effective unless the employees are aware of the expected security incidents and how to deal with them. The interviews suggest that this requires continual efforts from information security practitioners in making users' familiar, aware, and up-to-date with common threats, and potential damage associated with those threats. Training users in the detection of incidents, and swiftly responding as expected from them, includes ensuring they are able to make decisions on what security actions they should take, what procedures to follow, when, where, to whom, and how to report information security issues

.

- **Impact of the Information security culture**

The three categories provided above should be subject to periodic revisions and assessments to ensure their efficacy records kept of how awareness is monitored, evaluated, and maintained as a means of measuring its impact, not only on intended behaviour, but on actual behaviour. Experts have suggested that ongoing analysis of periodic reports would help keep track of the security culture within the organisation and help in detecting weakness in the awareness policy and procedures and correcting them accordingly. These reports include the number of employees properly following information security policies, the number of requests from different business units for information security awareness training and education programmes, the number of information security incidents, and the number of times employees violate compliance of the organisation's information security policy,

Figure 2 shows the framework for assuring information security awareness. The heart of the framework consists of fifteen mechanisms that should be tested as sub-areas of the four main focus elements. Together they make up assured information security awareness, in terms the organisational levels of knowledge, attitude, and behaviour. The right side of the framework represents the influencing factors. First, information security policy is assured by testing its accessibility, usability, clarity, and policy implications. Secondly, as users undergo awareness education and training, testing the security awareness material, delivery type and suitability. Actions to be taken by individuals during security incidents must be put into scenarios that reflect awareness of users and their readiness with a timely response. Lastly, the impact should be measured to be assured and improved.

4. Conclusion

Both the literature and the experts have confirmed that organisations recognise the importance of providing information security awareness programmes to their employees as an effective way to deter vulnerability and naive acts. However, there is a lack of measures to determine what is meant by effective programmes. This research provided essential measures of information

security culture for organisations in Middle East. The research framework in Figure 2 shows that the three constructs of knowledge, attitude, and behaviour, postulates that users' attitudes can be changed as they acquire knowledge. Such changes in attitude would result in changing their behaviour. Knowledge is acquired through involvement in a high level of information security culture, which that must be activated within employees' awareness, from foundations that are relied upon to prevent hacking attacks from within the organisations as well as from outside.

Many models and frameworks can be used to assess the level of information security awareness within organisations, but few are appropriate for all types of organisation. This paper has explained the reasons for proposing a framework that presents influencing factors for an effective information security awareness strategy within an organisation, which was confirmed by experts and practitioners.

It identifies the need for companies to focus on their individuals through the four elements of: information security policy, information security mechanisms, incident management, and the impact of those elements on the security culture level. In each case, it highlighted the various causes that specifically impact on the level of security awareness among individuals in Middle East organisations.

ACKNOWLEDGEMENT

We acknowledge Prince Sattam bin Abdul-Aziz University in Saudi Arabia and the Saudi Arabian Cultural Bureau in the UK for funding the scholarship for Fatima Almarshad that allowed the research to be undertaken.

References

[1] AbuSaad, B., Saeed, F., Alghathbar, K., Khan, B. (2011). Implementation of ISO 27001 in Saudi Arabia. In Proceedings of Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia. DOI 10.4225/75/57b52709cd8b2.

[2] Aydın, Ö. M., & Chouseinoglou, O. (2013). Fuzzy Assessment of Health Information System Users' Security Awareness. *Journal of Medical Systems*, 37(6), 9984.

[3] Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is Better Than Cure! Designing Information Security Awareness Programs to Overcome Users' Non-compliance with Information Security Policies in Banks. *Computers & Security*, 68: 145-159.

[4] Booth, D. A. (2015). Information Assurance for Small and Medium Enterprises (IASME)-3.0-2015, IASME Standard. Available at: http://iasme.co.uk/.

[5] Bruck, M. (2002). Security Threats from Within. Entrepreneur Europe. Online document at: http://www.entrepreneur.com/technology/newsandtrends/article50414.html

[6] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems*, 34(Special Issue 3), 523-548.

[7] Cardinali, R. (1995). Reinforcing our moral vision: examining the relationship between unethical behaviour and computer crime. *Work Study*, 44(8), 11-18.

[8] Danchev, D. (2003). Building and Implementing a Successful Information Security Policy. Available at: https://techgenix.com/building_implementing_security_policy/.

[9] Furnell, S., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computer and Security*, 25(1), 27-35.

[10] GDPR. (2018). Guide to the General Data Protection Regulation. Gov.uk. Available at: https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation.

[11] Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28(1), 75-105.

[12] HIPAA. (2021). What is 45 CFR § 164.530, #2? Available at https://www.hipaaguide.net/what-is-45-cfr-164-530/.

[13] ISACA. (2012). Processes for Essential Enterprise Security. https://www.isaca.org/cobit.

[14] ISO/IEC 27002-2013 IT Security Techniques. (2013). Code of practice for information security management, International Standards Organisation Available at http://www.iso.org/standard/54533.html.

[15] ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection. (2020). Governance of information security. Available at http://www.iso27001security.com/html/27014.html.

[16] Kazemi, M., Khajouei, H., & Nasrabadi, H. (2012). Evaluation of Information Security Management System success factors case study of municipal organizations. *African Journal of Business Management*, 6(14), 4982-4989.

[17] Kreicberga, L. (2010). International threat information security-countermeasures and human factors within SME, Master's dissertation, Sweden: Luleå University of Technology.

[18] Kruger, H. A., & Kearney W. D. (2006). A prototype for assessing information security awareness. *Journal of Computer Security*, 25(4): 289-296.

[19] Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. *Information Systems Frontiers*, 23(2), 361-373.

[20] McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151-156.

[21] Puhakainen, P. 2006. A Design Theory for Information Security Awareness, unpublished PhD Thesis, University of Oulu, Finland.

[22] SANS Institute. (2015). Glossary of Security Terms - Z. Retrieved from http://www.sans.org/security-resources/glossary-of-terms/?pass=z.

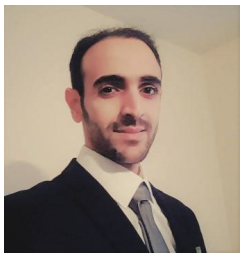
[23] Sewuster, P. (2013). Information security in practice, the practice of using ISO 27002 in the public sector. Master's Dissertation, University of Nijmegen. s4009126.
[24] Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. In Proceedings of new approaches to security, privacy and trust in complex environments, FIP/SEC7. Sandton, South Africa. 133-44.
[25] Sommers, K., & Robinson, B. (2004). Security awareness Training for Students at Virginia Commonwealth University. In Proceedings of the 32nd Annual ACM SIGUCCS Fall Conference on User services, USA New York, New York, ACM, 379-380.
[26] Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance, *Computers & Security*, 23(3), 191-198.

AUTHORS' CONTRIBUTIONS

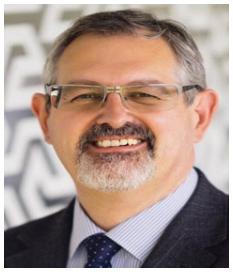
FA designed and developed the proposed framework, as well as confirming the framework by interviewing several experts. AA was involved in drafting the manuscript, while GW contributed to the Abstract and supervised FA. All authors read and approved the final manuscript.

INFORMATION ABOUT AUTHORS

Fatima Almarshad is a lecturer at Prince Sattam University, Saudi Arabia and a PhD candidate at the University of Southampton, UK. Fatima is interested in multidisciplinary research topics related to computer science. Her research area includes: Information Security standards, Information assurance, Security Risks, Security policies, security culture and awareness, and Internet of Things Security. Fatima's PhD research project focuses on Security and Information Assurance.



Abdullah I. A. Alzahrani PhD in Computer Science from the University of Southampton (United Kingdom, 2020), Master of Computer Information Systems (Information Security & Assurance) from Middle Tennessee State University (United States, 2016), Bachelor of Computer
Science from Taif University (Saudi Arabia, 2009), and Diploma in Computer Science (Programming Technology). Assistant Professor and the head of Computer Science Department at the College of Science and Humanities in Al-Quway'iyah, Shaqra University. His research interests are mainly focused on gamified e-learning, e-learning, information security and assurance, and human computer reaction.



Gary Wills is an Associate Professor in Computer Science at the University of Southampton. He graduated from the University of Southampton with an Honours degree in Electromechanical Engineering, and then a PhD in Industrial Hypermedia systems. He is a Chartered Engineer, a Member of the Institute of Engineering Technology, and a Principal Fellow of the Higher Educational Academy. He is also a visiting associate professor at the University of Cape Town and a research professor at RLabs. Gary's research projects focus on Secure System Engineering and applications for industry, medicine, and education.