
Article:
AlMindeel, R. and Martins, J.T. orcid.org/0000-0003-3906-5904 (2020) Information security awareness in a developing country context : insights from the government sector in Saudi Arabia. Information Technology & People. ISSN 0959-3845

https://doi.org/10.1108/itp-06-2019-0269

Title: Information Security Awareness in a developing country context: insights from the government sector in Saudi Arabia

Abstract

Purpose: The purpose of the article is to increase understanding of employee information security awareness in a government sector setting and illuminate the problems that public sector organisations in a developing context face when seeking to establish an information security awareness program.

Methodology: An interpretive research design was followed to develop an empirically enriched understanding of information security awareness perceptions, aspirations, challenges and enablers in the context of Saudi Arabia as a developing country. The study adopts a single case study approach including face-to-face interviews with senior employees as well as document analysis.

Findings: The paper theorises the importance of individual information security awareness, knowledge and behaviour and identifies a number of facilitating conditions: customisation to employee and organisational needs, interactivity, innovation, frequency, integration of both electronic and physical learning resources, and rewarding the acquisition of in-depth security-related actionable knowledge.

Originality: This study is one of the first to examine information security awareness as a socio-technical process within a government sector organisation in a developing country context.

Keywords: Information Security Awareness; Information Security Behaviour; Government sector; Public servants; Saudi Arabia

1. Introduction

Information security has become one of the basic operational requirements of any type of organisation, especially government organisations, and it entails safeguarding key information assets from security threats (e.g. unauthorised access, use, dissemination, corruption or destruction) that could endanger its availability, integrity and confidentiality (Gulappagol & ShivaKumar, 2017; Moon et al., 2018). In essence, the viable continuity and growth of organisations relies critically on assuring the confidentiality, integrity and availability of their informational assets (Rao & Nayak, 2014). In this context, organisations have progressively equipped themselves with different information security controls, namely administrative and technical security controls, in order to protect from as much security risks as possible. Examples of such controls would include information security awareness programmes as well as technical measures commonly known as network firewalls and virus detection systems (Johnson, 2015).

Individual actors are considered one of the indispensable elements of organisational information security. On the one hand, they are expected to be safely performing their given roles. That is the case, for instance, of a user interacting with their organisation's information system via authorised user accounts and passwords or also the case of an administrator continuously monitoring and managing the information security solutions employed by their organisation. On the other hand, individual actors could endanger the security status of an organisation through acts of negligence (Rao & Nayak, 2014). For instance, when an organisational insider clicks on a malicious link enclosed in an email, being unaware of the potential harm that can be caused by such a mistake (Jakobsson & Myers, 2006).

Given the complex nature of individual behaviour and the various dimensions of security vulnerability in organisational settings (Sebescen and Vitak, 2017), relying completely on

security-related technologies is insufficient to reduce all types of security risks and elevate the information security level of organisations in general. The insufficiencies of technical controls in a context where human intervention and insider threats (Ho et al, 2018) are so critical is well summarised by Schneier (2011) in the assertion that 'if you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology'. In this sense, the effective role of non-technical information security interventions, namely information security awareness, is emphasised by a variety of studies in the field (Bulgurcu et al. 2010; Haeussinger and Kranz, 2013, Siponen, 2000) as a form of deterrent information security measure (Tipton and Krause, 2007). More specifically, information security awareness involves making individuals aware of the importance of their conduct in relation to information security. In practice, such protective measures should be taken into consideration when planning and implementing the overall organisational security architecture (Rao and Nayak, 2014) and taking a realist and pragmatic stance (neither too utopian nor excessively dystopian), anchored on "evidence-based framing strategies" can help unpack information security as a complex socio-technical challenge (de Brujin and Janssen, 2017).

The limited existence of research in the domain of information security awareness focusing on governmental organisations has motivated Abraham's (2011) call for more scholarship to advance the understanding of information security behavioural factors in public sector and governmental settings. Within existing studies, such as Parsons et al.'s (2014) inquiry into Australian government organisations, it is found that employees' high level of knowledge in information security does not necessarily guarantee an adequate information security behaviour, which makes the case for an enhanced understanding of how information security awareness contributes to improve information security behaviour. Both contextually and geographically, there also seems to exist a bias towards Western contexts (Crossler, 2013) and

a lack of coverage of how information security as a grand societal challenge is experienced in developing countries, such as Saudi Arabia. Similarly, the studies that do focus on the Saudi Arabian context either identify the insufficiencies of information security awareness (Alarifi et al., 2012) or focus exclusively on information technology professionals, which may be understood to bias results (Alzamil, 2012).

Despite an increase in the use of information technologies across organisations, alongside the persistence of human behaviour-related threats such as social engineering (Hanus et al., 2018), limited action is taken to increase end users' information security awareness (Aloul, 2012). Few studies have empirically addressed information security awareness activities and their interactions with the various organisational processes and events. Some notable exceptions include: Albrechtsen and Hovden's (2010) identification that locally-based employee participation, group interaction/ reflection create changes in information security awareness and behaviour at individual level; Tsohou et al.'s (2012) examination of information security awareness as a managerial and socio-technical process within an organisational context; Ion et al.'s (2015) analysis of the discrepancies in the behaviour of security experts vs. non-security-expert internet users; McComarc et al's (2017) analysis of the relationship between individuals' information security awareness and variables such as gender, age, personality and risk-taking propensity; and Doherty and Tajuddin's (2018) exploration of the ways in which users' perceptions of information value influence their level of compliance with organisational information security policies. Though relatively nascent, this stream of research seems indicative of a growing recognition that technology alone is insufficient to deliver a complete information security solution (Furnell & Clarke, 2012; Abawajy, 2014), and that more attention should be dedicated to the confluence of behavioural and technological defences (Öğütçü et al., 2016; Safa et al., 2016). It is thus crucial to delve deeper in the appreciation of the socio-technical aspects surrounding information security awareness, notably employee aspirations

and perceived challenges and enablers in a developing context. In this context, the main aim of the article is to explore the various ways in which information security awareness influence employee security behaviour in government sector organisations, in the context of Saudi Arabia as a developing country. The aim is further specified in the following research questions: (a) in what manner do government sector employees perceive information security awareness initiatives to impact information security behaviour? (b) which factors do they perceive to operate as challenges and enablers of information security awareness? These questions are addressed through a case study of a government Agency in Saudi Arabia, and the empirical results position the contribution of the study within the field of information security behaviour research in general.

In terms of structure, the article is organised as follows. We begin with an identification of the different research foci on information security behaviour and information security awareness to develop a general picture of the field. We subsequently introduce the case and the data collection and analysis procedures employed. This is followed by a section in which the findings on government sector employees' experience and understanding of information security awareness are presented. Our findings are then discussed in light of previous research and we conclude the article with remarks on how they contribute to the information security awareness-related activities in the government sector.

2. The impact of information security awareness on information security behaviour

In today's growing security threat landscape, organisations should consider developing a protective shield to guard against internal information security risks initiated by employees' actions as well as external information security threats that might take advantage of employee's

negligent behaviour. A more security-aware workforce will protect organisations from falling into hackers' human-targeted traps (Siponen, 2000). In particular, social engineering, when used maliciously against organisations, is a considerable threat to employees, manipulating them into performing actions that could expose their organisation to serious security risks (Workman, 2008; Hadnagy, 2010). For instance, the consequences are dramatic when an attacker succeeds in obtaining sensitive information from employees by luring them to reveal secret personal information such as their user account / password in order to steal their network identity and gain unauthorised access to their organisation's systems. One common form of social engineering are phishing attacks, in which hackers create fake emails infected with malicious links and/or attachments and send them targeting an employee or group of employees. When performed in low volume and attacking specific users or employees of firms, organisations and governments, these attacks are known as spear phishing or whaling (Stembert et al., 2015). Successful attempts typically allow unsolicited access into the organisation's systems and can further establish a point of entry for more sophisticated security attacks (Hadnagy & Fincher, 2015). Ransomware breaches can also be the result of social engineering attacks. In this case, self-propagating malware uses encryption to hold a victim's data ransom until a payment is made. (Chen & Bridges, 2017). This was recently illustrated by the largescale WannaCry cyber-attack (Ehrenfeld, 2017), during which more than sixty National Health Service Trusts in the United Kingdom were prevented from accessing patient records, ultimately leading to costly delays and cancelations of non-urgent appointments and surgeries (Ghafur et al., 2019). In a work environment where the prevalence of these kinds of threats is becoming more common, enhancing employees' awareness level and associated protective behaviour (Jansson & von Solms, 2013) becomes crucial.

Studies focusing on the significance of organisations' information security awareness endeavours attribute its positive impact on individual information security behaviour in the

sense that the risk of employee negligence can be alleviated by employing a preventive approach (Bulgurcu et al., 2010; Haeussinger and Kranz, 2013) that mitigates risks originating both internally and externally (D'Arcy et al., 2009). A stream of behavioural psychology theories – including theory of planned behaviour, general deterrence theory (e.g. Workman and Gathegi, 2007) and protection motivation theory - has been traditionally used to quantitatively measure the impact of information security awareness on individuals' security-related conduct (Lebek et al., 2014). Drawing on theory of planned behaviour, Bulgurcu et al. (2010) explored the impact of employees' information security awareness level on their intention to exert a secure behaviour compatible with the organisation's information security policies, particularly by examining its influence on their attitude and its motivating factors. The findings firmly positioned information security awareness as one of the important predictors of employees' security-related behaviour through its positive relationship with employees' attitude. Similarly, and focusing on the identification of which factors matter the most for existence of security-compliant behaviour, Haeussinger & Kranz (2013) highlight the role of information security awareness initiatives – an argument already made by D'Arcy et al. (2009) when identifying information security misconduct deterrent measures.

A possible criticism of this family of studies is their use of behavioural psychology theories to establish conclusions on actual security behaviour when in effect what is being measured is the intention to 'comply' with or 'violate the organisation's security policies and guidelines (Bulgurcu et al., 2010; D'Arcy et al., 2009; Haeussinger & Kranz, 2013). Another branch of studies has attempted to measure the significance of various internal and external factors on employees' behaviour, which helped identifying the set of factors influencing employees' information security awareness levels (Chen et al., 2012; D'Arcy & Devaraj, 2012; Herath & Rao, 2009a; Herath & Rao, 2009b; Hu etal. 2012; Ifinedo, 2012; Siponen et al., 2014). More recently, factors such as attentional and motor impulsivity have been identified as significant

positive predictors of risky cybersecurity behaviours, whereas individual features such as openness to experience, honesty and agreeableness were found to correlate with lower risk taking and higher information security awareness (Hadlington, 2017). In general terms, this branch of studies has provided mostly a quantitative evaluation of employees' information security awareness level with some variation in organisational contexts and selected theoretical constructs (Alsaif et al., 2015; Chan and Mubarak, 2012, Parsons et al. 2014), but nevertheless with an emphasis on private sector organisations.

3. Factors influencing employees' information security awareness

Knowing the set of internal and external factors that can positively influence awareness levels is essential in understanding information security awareness initiatives in organisations and their effect on individuals' security behaviour (Bulgurcu et al, 2010; Haeussinger & Kranz , 2013; Chen et al., 2012; D'Arcy and Devaraj, 2012; Herath & Rao, 2009a; Herath & Rao, 2009b; Hu et al., 2012; Ifinedo, 2012; Siponen et al., 2014). Internal and motivational factors influencing employees' information security awareness level and ultimately their security behaviour are mainly attributed to their predisposition towards conforming with existent information security policies, their commitment to the organisation's security resources as well as their previous encounter with information security issues and threats (Bulgurcu et al, 2010; Haeussinger & Kranz, 2013; Herath & Rao, 2009b). The notion that a successful information security awareness programme must be based on improving employees' cognitive frames of reference is well established (Thomson and von Solms, 1998), especially when training is problem-centred (Pawlowski et al., 2015) and designed with an emphasis on appropriate security practices that improve online behaviour (McChrohan et al., 2010), therefore aiming at reducing organisational insiders' cyber risk behaviour (Bulgurcu et al, 2010; Hu et al., 2012;

Herath & Rao, 2009b). Empirical evidence in several studies has proven the strong connection between employees' attitude and their behavioural intention to display information security-aware behaviour. Therefore, employee attitude often emerges in the information security literature as one of the main constructs when examining information security awareness within organisations (Bulgurcu et al, 2010; Haeussinger and Kranz, 2013; Parsons et al., 2014). Of special relevance is employees' level of organisational commitment - translated into the predisposition to behave within the organisation's framework of accepted security behaviour (Herath and Rao, 2009b) – and the existence of some form of experience with information security, which will impact future security behaviour and induce increased levels of consciousness, threat awareness and knowledge of remedial actions (Bulgurcu et al., 2010; Haeussinger and Kranz, 2013).

At organizational level, other factors such as organisational culture, leadership (Siponen, 2000; Connolly et al., 2017; Hu et al., 2012) and the existence of reward and sanction mechanisms (Bulgurcu et al., 2010; Chen et al., 2012; Herath & Rao; 2009a) are also found to induce employees to comply with recommended information security behaviour. Organisations' concern with the fulfilment of their members is related to an increase in employee loyalty and perceived sense of attachment, which in turn promotes adequate security conduct amongst organisational members, expressed also as concern for the security the organisation's information resources and an open stance towards discussion information security challenges and avoidance strategies. Top management support is critical for the solidification of this type of organisational culture (Hu et al., 2012). Enabling ingredients of a well-developed organizational information security awareness are also found in reward and sanction mechanisms, although with some polarised views of which mechanisms operate as key determinants and some studies (e.g. Herath & Rao, 2009a) arguing for the effectiveness of

sanctions as a deterrent of misconduct, whilst others advocate the role of rewards in positively shaping employees' security compliant behaviour (Chen et al., 2012).

4. Methods and Data

We followed an interpretive research epistemology and adopted a case study approach (Denzin and Lincoln, 2000) for this study. The empirical methods for data collection included document analysis and semi-structured interviews. The data were analysed with inductive data analysis techniques (Braun & Clarke, 2006).

The study was conducted at a Saudi Arabia government Agency established by Royal Decree and with a strategic remit to plan and oversee urban, energy infrastructure and environmental development. Interview participants consisted of fifteen senior employees originating in the various departments that compose the organisation, as depicted in Figure 1 below. The sampling of senior employees is an acknowledgement that there are managerial, strategic, and financial considerations in every organisation's best efforts to become cybersecure. This means that, in terms of information security awareness, minimising exposure to information security hazards is not just the responsibility of the IT department – it is every department's job. The diverse roles of these senior managers provide unique insights into the production and integration of information security awareness perspectives at organisational level, especially how information conversations across teams and workplace colleagues develop, how risk is assessed, how defences are improved and how overall decision-making to enhance information security is made.

Following the principle of identifying an information-rich setting, the selection of the case was paradigmatic (Flyvbjerg, 2007), given the study's focus on exploring employee information

security awareness in a government-sector organisation. Similar to other initiatives promoted by governments in different regions of the globe (e.g. the UK's National Cyber Security Centre or Germany's Federal Office for Information Security), the Ministry of Communications and Information Technology (MCIT) in Saudi Arabia has issued a National Information Security Strategy (NISS) in 2011 yielding several key recommendations that ought to be implemented to increase increasing information security awareness (Ministry of Communications and Information Technology, 2011). Moreover, following the country's 2030 vision, investment on digital infrastructure has increased rapidly (Alshuaibi, 2017). More importantly, due to recent security incidents, the country's spending on information security has increased as well. For instance, the government has established the National Cyber Security Center (NCSC) for the sole purpose of strengthening the country's information security position (Hathaway et al., 2017).

INSERT FIGURE 1 HERE

The participants, profiled in Table 1, are characterised in terms of their organisational affiliation as core members and by their professional nomenclatures. They have all undergone mandatory information security awareness training offered by the Agency. In order to maintain the confidentiality of participants, alias names have been created and assigned to each interviewee.

INSERT TABLE 1 HERE

The information security policy documents produced by the Agency – summarised in Table 2 - were also collected to perform cross-analysis against the data collected via the interviews, which allowed the developed of further insights into the role and practice of information security awareness.

INSERT TABLE 2 HERE

This level of identification was considered sufficient to conduct the analysis of data and respects the research confidentiality parameters agreed by participants in consent forms prior to the study and approved by the Research Ethics Committee of the University of Sheffield. The interviews were conducted over a period of two months (see Appendix 1 for the interview guide). They lasted on average fifty minutes and were audio-recorded and transcribed by the first author.

To select interviewees and policy documents, we used theoretical sampling (Eisenhardt 1989). The selection was based on the initial research topic and objectives, and the aim was to present a real-world case that transparently represents the phenomenon under study (Eisenhardt and Graebner, 2007).

Both the policy documents and interview data were manually analysed following inductive thematic analysis (Braun & Clarke, 2006) and its stages of understanding data, developing codes and identifying themes, which are reported in the 'Results' section. Following this inductive process of data analysis allowed the researchers to read and re-read through policy documents and interview transcripts, assign initial codes, note connections, look for themes and work through them in terms of internal consistency and external heterogeneity. The analysis was a process of interaction and refinement, co-developed by the two researchers, until a shared sense of analytical saturation was achieved.

More specifically, as prescribed by Braun and Clarke (2006), the researchers read and re-read each interview transcript and policy document to familiarise themselves with the data; (2) produced initial codes systematically across the data set; (3) collated initial codes into potential themes; (4) refined themes based on internal homogeneity and external heterogeneity (Patton,

1990); (5) and defined and labelled final themes. The iterative process of comparing and linking themes proceeded to generating an illustrative framework that is representative of the analysis, presented in synthesis in Table 3 below and in detail in the 'Results' section of the article.

INSERT TABLE 3 HERE

Internal validity of data was strengthened through the use of constant comparison (Silverman, 2000). Saturation occurred when new codes failed to emerge from the data. The reliability of the analysis was sought through the collaborative development of coding and identification of themes between the authors, who followed the principle of consensus in order to attain interpretive agreement and reliability.

5. Results

5.1 Perceived impact of information security awareness

Information security awareness is considered as a protection factor against employees' potential lack of knowledge about security threats they might fall victim to, without proper identification or detection in advance: "ISA is about employee's knowledge of the vulnerabilities or mistakes through which the system is breached, such as electronic phishing emails" (Qadir, Information Systems Coordinator). This is especially important in the context of the organisation's duty of safeguarding citizens' personal and financial data, as expressed in policy:

> "The user shall not reveal or publicise confidential or proprietary information which includes, but not limited to: financial information, contract & projects,

> investment opportunities, organizational strategies and plans, databases and the information contained therein (…)" (IU2013).

The internalisation of this duty was acknowledged by most participants as a continuous reminder that information security awareness is a dynamic knowledge process. In that sense, information security awareness is perceived as an opportunity to increase employees' knowledge about the organisation's policies and guidelines, therefore fulfilling an educational role, in the sense that it "[informs] people about the policies and procedures that are being used in terms of information security and information crimes" (Ghazi, Project Manager). Ideally, it should become an effective generator of good habits and ultimately a culture of operational safety, where the possibility of vulnerability is minimised and controlled:

> "(…) if the institute stimulates employees, they will be motivated automatically. If there is information continuously, then people will get used to it and start adapting to it normally. It becomes a kind of reminder every time, employees then obtain related information and background and with time it becomes a culture" (Fadil, Human Resources Manager).

Achieving that state requires systematising the information dissemination beyond irregular communication efforts, in order for information security awareness to attain impact and operate effectively as an active reminder of security-related behaviour, recommendations, guidelines, potential security threats, and possible ways to overcome them:

> "Frankly there is an impact. On my junk email I receive emails but before I open any I make sure that if there is a link or something to be opened and since my job entails dealing with investors. I make sure before I open it that it came from the

right email address so now I would say there is more consciousness (…)" (Daoud, CEO Officer Advisor).

5.2 Desired impact of information security awareness

The success of information security awareness initiatives was perceived by mostly employees to rely on effective planning and alignment with workplace activities, so that it becomes "an acceptable mechanism that does not negatively impact work" (Salim, Human Resources Director). In, turn, such initiatives would enable comprehensive knowledge in terms of information security including information about possible security threats that could be faced by non-IT employees as well as information about required information security policies and guidelines. The foundations for this knowledge are understood to lie with formal, immersive and experiential security training:

> "A deeper approach would be to include an internal course which allows for learning in a deeper and wider way. Besides it gives a chance to the employee to ask questions, respond and experiment." (Qadir, Information Systems Coordinator)

The emphasis on experimentation conveys the aspiration for content that clearly reflects the real security dangers and the necessary precautions and mitigating actions, which are only accessible when employees are "engaged in the problem (…) and know the real damage, something concrete!" (Jamal, Executive Spokesperson). This endeavour is facilitated by the regular assessment of employees' information security awareness level, to allow the identification of necessary improvements (Abbas, Support Services Director).

Besides formal learning approaches, employees expressed interest to learn through non-traditional learning methods, including self-learning and the use of digital resources. For instance, learning gained through e-learning courses, electronic quizzes, and simulated

phishing attacks were reported to be “more attractive and engaging” (Jamal, Executive Spokesperson), “easier to recall” (Farida, Trainer-Assessor), and likely to “encourage conversation between employees” (Jamal, Executive Spokesperson). Such desired impact indicates employees’ willingness to utilise more innovative and interactive learning approaches.

In addition to more innovative ways to learn about information security, the impact of awareness materials is perceived to be greater if it is expanded into a more organised effort where a variety of awareness materials is quickly mobilised and accessed, such as in the case of periodicals, “electronic materials that can be easily shared with others” (Masud, Industrial Coordinator), campaigns, events or the use of social media, for instance:

> “Twitter hashtags where its impact would be very strong particularly if used as part of a campaign or using the 5-10 seconds YouTube adds as a reminder which would have a bigger impact and another example would be campaigns in Snapchat, which nowadays became a very attractive tool” (Saida, Analytics Consultant).

Although the convenience of electronic interactions is praised by most employees, face-to-face interaction with IT personnel is still considered relevant, particularly in maintaining a meaningful relationship with staff members and providing reassurance of personalised, dedicated and responsive action. This kind of response entails more dedication than brief encounters with IT support on a trouble-shooting basis:

> "For instance, if something happens, someone from the IT department comes to check your device only for a few minutes and then disappears. He doesn’t explain the issue or how it happened and how we can avoid it or what was our mistake?" (Masud, Industrial Coordinator).

5.3 Perceived challenges and enablers of information security awareness

Employees have collectively highlighted several factors in relation to their internal value system, which they perceived to have an impact in their information security-related behaviours. Amongst these factors, a sense of individual responsibility towards contributing to the Agency's security was frequently alluded to as an integral component of their professional ethos: "It is always someone's values what will top everything else; therefore, a person will care about information security for that reason first and foremost." (Tarek, Inspector).

This stance, where a concern for security is taken as a common denominator of government sector workers' professional praxis, leads to a very negative framing of organisational attempts to punish noncompliance and misconduct. Consequences in terms of professional progression are particularly unwelcome and the use of rewards as incentives of good citizen behaviour is preferred:

> "In my opinion, sanctions would have an impact, but it would be a negative one since no one likes punishment. I had a say in it, I would avoid sanctions as much as possible. I would mostly concentrate on awareness and rewards, even if symbolic" (Masud, Industrial Coordinator).

A minority of employees sees some "disciplining value through corrective action" (Omar, Economist) in the application of sanctions, but most participants argue that the emphasis should be on substantiating workers' knowledge base through information security awareness initiatives and, in particular, to provide advanced information technology skills. Knowing how to deal with information systems is essential in enabling employees to identify the possible security risks, assess them correctly and ultimately be able to conceptualise the related

damages, which indicates a logical nexus between employees' computer skills and their vulnerability towards information security attacks:

> "The first thing that employees need to have is a solid level of information technology skills, in order to have a grasp of the possible loopholes and risks that could be faced. The more an employee is ignorant with regards to IT, the more easily he/she can be attacked" (Imad, Customer Support Coordinator).

An important opportunity to further absorb information security-related knowledge lies with workers' first-hand experiences. Personal experiences with information security typically involve identifying the perceived threat, searching for information about the incident and most, importantly, choosing a suitable response such as avoidance or directly seeking support. Such threat-response situations are real life experiences that will have significant impact not only on employee's reception of information security awareness initiatives but also - if guided properly – will convert employees into indirect promoters of information security in the Agency:

> "There were signs. I have received couple of them repeatedly. When I asked about them, I was told that those are… some form of breach used for spying or causing harm. For instance, someone sends an email and it has a link or a fake attachment. I later realised that this is called phishing. The important thing is that I have not opened the enclosed attachment and did not forward the email and reported the issue, to be shared" (Masud, Industrial Coordinator).

Knowing about issues that had happened to other co-workers was perceived by most participants to be beneficial in developing critical awareness about experienced threats and related responses and in consolidating an organisational culture that is security-focused.

6. Discussion

The information security literature has, in general terms, emphasised the importance of employees' attitudes and behavioural intentions as predictors of actual information security compliance (Bulgurcu et al., 2010; Hu et al., 2012; Herath & Rao, 2009b). Focusing specifically on the government-sector, our analysis reveals that employees perceive information security awareness as a form of protection against risks associated with information security misconduct, which aligns with existing literature that positions information security awareness as a deterrent from insider threats (D'Arcy et al., 2009).

The experience of risks and threats is generally claimed to play a useful role in shaping a more acute information security awareness and adopting a more vigilant stance (Bulgurcu et al., 2010; Haeussinger and Kranz, 2013). More than actually falling victim to information security attacks, employees in the case government organisation value the experience of peers who have been exposed to threats and successfully dodged them, as it allows them to model behaviour on how to handle and report such incidents.

In this sense, information security awareness is viewed as a precautionary measure to avoid risks in relation to employees' negligence of recommended security conduct. It requires planning and formalisation to ensure the effective allocation of resources (Desman, 2001; Siponen, 2000; Thomson and von Solms, 1998). Indeed, in the case government organisation there is self-acknowledged recognition of a positive impact of information security awareness in individual information security behaviour, which echoes the perceptions of employees in private sector organisations where the positive impact of information security awareness endeavours on the intention to exert security compliant conduct has also been found (Bulgurcu et al., 2010; Haeussinger and Kranz, 2013; Choi et al., 2018).

However, this study extends prior literature by providing novel insights into specific requirements identified regarding the effectiveness of current organisational information security awareness and the calls for more knowledge-focused activities, indicating strong information security-specific knowledge acquisition aspirations. This finding adds a new perspective to Siponen's (2000) argument that, in order to guarantee a positive impact of information security awareness on employees, it is necessary to convince them of the necessity to abandon or adhere to a certain security act through reason and argument. Such convincing, we argue, operates through employees' agency and ability to access satisfactory knowledge that will allow them to practically apply the gained information both at work and in their personal lives.

Agency is particularly important even if top-management support is widely acknowledged as an enabler, especially at the levels of compliance behaviour and security controls implementation (Siponen, 2001; Hu et al., 2012), although not always experienced to the desired extent, in practice.

Contrary to claims in the literature (D'Arcy et al., 2009), managerial action at the levels of sanctioning misconduct and information security policy violation is perceived by employees at the case government organisation to be detrimental to employees' commitment, especially if there is an impact on performance evaluation, which may engender feelings of resentment and disengagement. Nevertheless, employees perform what Bulgurcu et al. (2010) describe as an assessment of behaviour costs and benefits and are mindful of its consequences. They instead prefer information security awareness initiatives that emphasise the use of rewards (Chen et al., 2012) as an instrument to draw employees' attention and entice them to acquire more knowledge on information security. This type of emphasis on the use of rewards gives

information security a face (de Brujin and Janssen, 2017) and puts the employees, natural organisational allies, in the spotlight.

A fundamental component of that knowledge base comprises sophisticated computer security skills that enable employees to distinguish potential security threats, anticipate their impact and initiate suitable responses. This requires, on the one hand, embedding security training in government organisations' information security awareness efforts and, on the other hand, designing suitable learning experiences, content, forms of communication as well as planning and evaluation instruments. Haeussinger and Kranz (2013), have demonstrated that, among other factors, employing information training programs within private sector organisations has a substantial influence on employees' awareness and information security conduct, to the extent that it may impede internal members from behaving against the organisation's interest. Similarly, D'Arcy et al. (2009) have shown that information security awareness training can dissuade employees from acts of misconduct that could jeopardize their organisation's information security strategy. This study extends this line of inquiry by providing insights into specific requirements identified for a government sector organisation. These include customisation to employees' and organisational needs, interactivity, innovation, frequency and the integration of both electronic and physical learning resources.

Interestingly, employees in the case government organisation have shown great desire for in-depth and formal training approaches accompanied by one-to one communication with information security awareness professionals. Yet, they have also revealed willingness for more innovative and interactive, computer-based learning approaches, mainly due to the perceived novelty and flexibility of such approaches. Both approaches reflect the preferences and needs of government employees towards information security awareness learning and training efforts. In recent years, the information security literature has shown interest in

electronic and interactive security training methods such as e-learning and game-based training programs where a positive impact on individuals' information security knowledge and behaviour is observable. For instance, Hagen & Albrechtsen (2009) tested the perceived impact of information security e-learning programmes on private sector employees to identify substantial improvements in their information security awareness levels, namely knowledge and behavioural aspects. However, a later study (Hagen et al., 2011) revealed that the long-term impact of such programs has declined over time, particularly in relation to employees' gained knowledge, which signals the necessity of frequent training initiatives. This assertion strengths the call made by the case government organisation employees' for the regular frequency and compulsory nature of information security training and awareness raising activities.

Moreover, employees' desire for electronic means of communication is not restricted to training activities and is also reflected in their preferred awareness channels namely electronic mails as well as their preference for non-printed awareness materials over printed ones. This extends current knowledge on digital information security learning methods (Cone et al., 2007) and places it within the specific context of government organisations.

Finally, and remaining true to what they consider to be a learning process, employees have expressed the need for an evaluation mechanism so they could obtain formal feedback on their information security awareness level. This resonates with the practice of private sector organisations, where evaluation has been highlighted as a key element in the design and implementation of effective information security awareness programs (Desman, 2001; Hansche, 2001; Peltier, 2005), especially through the use of phishing simulations (Dodge et al., 2007; Jansson & von Solms, 2013).

We acknowledge that our interpretive approach cannot aim at producing generalisable explanations (Orlikowski and Baroudi, 1991), because it is primarily focused on producing an understanding of the context and the processes (Walsham, 1995) of information security awareness as intersubjectively experienced in the case organisation. However, the regularities observed in the context of this Saudi governmental agency have implications beyond the studied research setting and a number of recommendations is analytically transferable to other governmental agencies in developing countries:

1. Commitment to effective planning in terms of formalised information security awareness activities as well as the need for more engaging activities. Conducting security awareness campaigns which combine the impact of various awareness materials with the organisation's needs to effectively promote its information security capabilities is a recommended practice;
2. A mixed learning approach is recommended to satisfy preferences for both face-to-face interaction as well as electronic self-learning approaches. In addition, given the prospect of declining long-term impact of information security e-learning courses, it is recommended that information security awareness training activities are institutionalised as mandatory and regular;
3. The implementation of formal evaluations methods including simulations and questionnaires is vital to determine employees' information security awareness levels and extract feedback for the re-design and continuous improvement of information security awareness training interventions.

7. Conclusions

The use of an interpretative research design, as in the current study, is still unusual in the context of information security awareness research in government sector organisations and, in addition, in the context developing countries. By investigating employees across the various departments of a Saudi government Agency, our objective was to illuminate the role played by information security awareness in government-sector employees' information security behaviour from an empirically enriched perspective, and with an explicit focus on information security awareness perceptions, aspirations, challenges and enablers.

As governmental organisations in developing countries become increasingly information-intensive and digitalised, the ways in which the development studies and information science communities examine information security awareness become increasingly important for understanding the complex contextualised information security management practices, including their processes and inherent interactions.

Turning to our specific findings, the study indicates that employees perceive information security awareness as a form of protection against risks associated with information security misconduct. Theoretically, this highlights employee agency and determination to access satisfactory knowledge – mostly through blended forms of training and peer exchange - that will allow them to practically apply the gained information both at work and in their personal lives. In a similar fashion emphasising agency and challenging existing assumptions, the sanctioning of misconduct and information security policy violations are perceived to be detrimental to employees' commitment and sense of engagement. Conversely, the effectiveness of information security awareness activities is found to be reinforced, amongst other factors, by: customisation to employee and organisational needs, interactivity,

innovation, frequency, integration of both electronic and physical learning resources, and rewarding the acquisition of in-depth security-related actionable knowledge.

Although our study is context specific and we do not claim the specific results to be generalisable, they illustrate a more generally plausible assertion concerning the relevance and implementation of information security awareness activities within government-sector organisations in developing countries. They place individual employees' aims and preferences in a wider organisational context and help to explain why organisational members take certain preferences and actions. We hope that our proposed type of theorisation - rare in the mainstream information security research, more accustomed to the deductive application of theory to empirical settings – adds to the ongoing development of the information security awareness research direction.

References

Abawajy, J. (2014), "User preference of cyber security awareness delivery methods", *Behaviour & Information Technology*, Vol. 33 No. 3, pp. 237-248.

Abraham, S. (2011), "Information security behaviour: factors and research directions", paper presented at the *Americas Conference on Information Systems* (2011), available at https://aisel.aisnet.org/amcis2011_submissions/?utm_source=aisel.aisnet.org%2Famcis2011_submissions%2F462&utm_medium=PDF&utm_campaign=PDFCoverPages (accessed 10 May 2019).

Albrechtsen, E., & Hovden, J. (2010), "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers & Security*, Vol. 29 No. 4, pp. 432-445.

Aloul, F. A. (2012), "The need for effective information security awareness", *Journal of Advances in Information Technology*, Vol. 3 No. 3, pp. 176–183.

Alshuaibi, A. (2017), "Technology as an Important Role in the Implementation of Saudi Arabia's Vision 2030", *International Journal of Business, Humanities and Technology*, Vol. 7 No. 2, pp. 52-62.

Alzamil, Z. A. (2012), "Information Security Awareness at Saudi Arabians' Organizations: An Information Technology Employee's Perspective", *International Journal of Information Security and Privacy,* Vol. 6 No. 3, pp. 38-55.

Alarifi, A., Tootell, H., & Hyland, P. (2012), "A study of information security awareness and practices in Saudi Arabia", paper presented at the *International Conference on Communications and Information Technology* (2012), available at https://ieeexplore.ieee.org/abstract/document/6285845 (accessed 10 May 2019).

Alsaif, M., Aljaafari, N., & Khan, A. R. (2015), "Information Security Management in Saudi Arabian Organizations", *Procedia Computer Science*, Vol. 56, pp. 213-216.

Braun, V., & Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Chan, H., & Mubarak, S. (2012), "Significance of information security awareness in the higher education sector", *International Journal of Computer Applications*, Vol. 60 No. 10, pp. 23-31.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012), "Organizations' information security policy compliance: Stick or carrot approach?", *Journal of Management Information Systems*, Vol. 29 No. 3, pp. 157-188.

Chen, Q., & Bridges, R. A. (2017), "Automated behavioral analysis of malware: A case study of wannacry ransomware", In *2017 16th IEEE International Conference on Machine Learning and Applications,* pp. 454-460.

Choi, S., Martins, J. T., & Bernik, I. (2018) "Information security: Listening to the perspective of organisational insiders", *Journal of Information Science*, Vol. 44 No. 6, pp. 752–767.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007), "A video game for cyber security training and awareness", *Computers & Security*, Vol. 26 No. 1, pp. 63-72.

Connolly, Y., Lang, L. Gathegi, M. J., & Tygar, D. J. (2017), "Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study", *Information & Computer Security*, Vol. 25 No. 2, pp. 118-136.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32, pp. 90-101.

D'Arcy, J., & Devaraj, S. (2012), "Employee misuse of information technology resources: Testing a contemporary deterrence model", *Decision Sciences*, Vol. 43 No. 6, pp. 1091-1124.

D'Arcy, J., Hovav, A., & Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98.

de Bruijn, H., & Janssen, M. (2017), "Building cybersecurity awareness: The need for evidence-based framing strategies", *Government Information Quarterly*, Vol. 34 No. 1, pp. 1-7.

Denzin, N.K., & Lincoln, Y.S. (2000), *Handbook of qualitative research*, Sage, Thousand Oaks, CA.

Desman, M. B. (2001), *Building an information security awareness program*, Auerbach Publications, New York.

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007), "Phishing for user security awareness", *Computers & Security*, Vol. 26 No. 1, pp. 73-80.

Doherty, N. F., & Tajuddin, S. T. (2018), "Towards a user-centric theory of value-driven information security compliance", *Information Technology & People*, Vol. *31* No. 2, pp. 348-367.

Eisenhardt, K. M. (1989), "Building theories from case study research", *Academy of Management Review*, Vol. 14 No. 4, pp. 532-550.

Eisenhardt, K. M., & Graebner, M. E. (2007), "Theory building from cases: Opportunities and challenges", *Academy of Management Journal*, Vol. 50 No. 1, pp. 25-32.

Flyvbjerg, B. (2007), "Five misunderstandings about case-study research", in Seale, C., Gobo, G., Gubrium, J. F. & Silverman, D. (Eds.), *Qualitative Research Practice*, Sage, London, pp. 390-404.

Furnell, S., & Clarke, N. (2012), "Power to the people? The evolving recognition of human aspects of security", *Computers & Security*, Vol. 31 No. 8, pp. 983-988.

Ghafur, S., Grass, E., Jennings, N. A., & Darzi, A. (2019), "The challenges of cybersecurity in health care: the UK National Health Service as a case study", *The Lancet Digital Health*, Vol. 1 No. 1, e10-e12.

Gulappagol, L., & ShivaKumar, K. B. (2017), "Secured data transmission using knight and LSB technique". In *2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, pp. 253-259.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, Vol. 3, no. 7, e00346.

Hadnagy, C. (2010) *Social engineering: The art of human hacking*, John Wiley & Sons, London.

Hadnagy, C., & Fincher, M. (2015) *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*, John Wiley & Sons, London.

Haeussinger, F., & Kranz, J. (2013) 'Information security awareness: Its antecedents and mediating effects on security compliant behavior'. Paper presented at the *International Conference on Information Systems*, Milan, Italy (2013), available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.669.8230&rep=rep1&type=pdf (accessed 10 May 2019).

Hagen, J. M., & Albrechtsen, E. (2009), "Effects on employees' information security abilities by e-learning", *Information Management & Computer Security*, Vol. 17 No. 5, pp. 388-407.

Hagen, J., Albrechtsen, E., & Ole Johnsen, S. (2011), "The long-term effects of information security e-learning on organizational learning", *Information Management & Computer Security*, Vol. 19 No. 3, pp.140-154.

Hansche, S. (2001), "Designing a Security Awareness Program: Part 1", *Information Systems Security*, Vol. 9 No. 6, pp. 1-9, DOI: 10.1201/1086/43298.9.6.20010102/30985.4

Hanus, B., Windsor, J. C., & Wu, Y. (2018), "Definition and multidimensionality of security awareness: close encounters of the second order", *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, Vol. 49, pp. 103-133.

Hathaway, M. Spidalieri, F. & Alsowailm, F. (2017), "Kingdom of Saudi Arabia Cyber Readiness at a Glance", available at http://www.potomacinstitute.org/images/CRI/CRI2_0_SaudiArabiaPofile.pdf. (accessed 10 May 2019).

Herath, T., & Rao, H. R. (2009a), "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165.

Herath, T., & Rao, H. R. (2009b), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125.

Ho, S. M., Kaarst-Brown, M., & Benbasat, I. (2018), "Trustworthiness attribution: Inquiry into insider threat detection", *Journal of the Association for Information Science and Technology*, Vol. 69 No. 2, pp. 271-280.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012), "Managing employee compliance with information security policies: The critical role of top management and organizational culture", *Decision Sciences*, Vol. 43 No. 4, pp. 615-660.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31 No. 1, pp. 83-95.

Ion, I., Reeder, R., & Consolvo, S. (2015), "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices, In *Eleventh Symposium On Usable Privacy and Security,* pp. 327-346.

Jansson, K., & von Solms, R. (2013), "Phishing for phishing awareness", *Behaviour & Information Technology*, Vol. 32 No. 6, pp. 584-593.

Jakobsson, M., & Myers, S. (2006), *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*, John Wiley & Sons, London.

Johnson, L. (2015), *Security Controls Evaluation, Testing, and Assessment Handbook*, Syngress, Waltham.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014), "Information security awareness and behavior: A theory-based literature review", *Management Research Review*, Vol. 37 No. 12, pp. 1049-1092.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017), "Individual differences and information security awareness", *Computers in Human Behavior*, Vol. 69, pp.151-156.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010), "Influence of awareness and training on cyber security", *Journal of internet Commerce*, Vol. 9, No. 1, pp. 23-41.

Ministry of Communications and Information Technology (2011), "Developing National Information Security Strategy for the Kingdom of Saudi Arabia". Available at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_EN.pdf (accessed 10 May 2019).

Moon, Y. J., Choi, M., & Armstrong, D. J. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. *International Journal of Information Management*, Vol. 40, pp. 54-66.

Nayak, U., & Rao, U. H. (2014), *The InfoSec handbook: An introduction to information security*, Apress, Berkeley, CA.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016), "Analysis of personal information security behavior and awareness", *Computers & Security*, Vol. 56, pp. 83-93.

Orlikowski, W. J. and Baroudi, J. J. (1991), "Studying Information Technology in Organizations: Research Approaches and Assumptions", *Information Systems Research*, Vol. 2 No. 1, pp. 1-27.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014), "A study of information security awareness in Australian government organisations", *Information Management & Computer Security*, Vol. 22 No. 4, pp. 334-345.

Patton, M. Q. (1990), *Qualitative evaluation and research methods*. Sage Publications, London.

Pawlowski, S. D., & Jung, Y. (2019), "Social representations of cybersecurity by university students and implications for instructional design", *Journal of Information Systems Education*, Vol. 26 No. 4, pp. 281-294.

Peltier, T. R. (2005), "Implementing an Information Security Awareness Program", *Information Systems Security*, Vol. 14 No. 2, pp. 37-49.

Safa, N. S., Von Solms, R., & Futcher, L. (2016), "Human aspects of information security in organisations", *Computer Fraud & Security*, Vol. 2, pp. 15-18.

Schneier, B. (2011) *Secrets and lies: digital security in a networked world*, John Wiley & Sons, London.

Sebescen, N., & Vitak, J. (2017), "Securing the human: Employee security vulnerability risk in organizational settings", *Journal of the Association for Information Science and Technology*, Vol. 68 No. 9, pp. 2237-2247.

Silverman, D. (2000) *Doing qualitative research: A practical handbook*. London: Sage.

Siponen, M. T. (2000), "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*, Vol. 8 No. 1, pp. 31-41.

Siponen, M. T. (2001), "Five dimensions of information security awareness", *Computers and Society*, Vol. 31 No. 2, pp. 24-29.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014), "Employees' adherence to information security policies: An exploratory field study", *Information & Management*, Vol. 51 No. 2, pp. 217-224.

Stembert, N., Padmos, A., Bargh, M. S., Choenni, S. and Jansen, F. (2015),"A Study of Preventing Email (Spear) Phishing by Enabling Human Intelligence," *2015 European Intelligence and Security Informatics Conference*, Manchester, 2015, pp. 113-120.

Thomson, M. E., & von Solms, R. (1998), "Information security awareness: educating your users effectively", *Information Management & Computer Security*, Vol. 6 No. 4, pp. 167-173.

Tipton, H., & Krause, M. (2007) *Information Security Management Handbook* (6th ed.), Taylor & Francis, Boca Raton, FL.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012), "Analyzing trajectories of information security awareness", *Information Technology & People*, Vol. 25 *No.* 3, pp. 327-352.

Walsham, G. (1995), "Interpretive case studies in IS research: nature and method", *European Journal of Information Systems*, Vol. 4, pp. 74-81.

Workman, M. (2008), "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security", *Journal of the American Society for Information Science and Technology*, Vol. 59 No. 4, pp. 662-674.

Workman, M., & Gathegi, J. (2007), "Punishment and ethics deterrents: A study of insider security contravention", *Journal of the American Society for Information Science and Technology*, Vol. 58 No. 2, pp. 212-222.

Table 1 – Profile of participants

Interviewee		Affiliation	Job title	Age	Gender	Years of experience	IT skills
1	Masud	Planning & Development	Industrial Coordinator	25 – 29	M	5 - 10	Good
2	Qadir		Information Systems Coordinator	25 – 29	M	< 5	Excellent
3	Adil		Environmental Consultant	25 – 29	M	< 5	Excellent
4	Umar	Finance	Auditing Specialist	35 – 39	M	> 10	Good
5	Omar	Technical Affairs	Economist	30 – 34	M	5 - 10	Excellent
6	Abbas	Support Services	Director	25 – 29	M	5 - 10	Excellent
7	Imad		Customer Support Coordinator	30 – 34	M	> 10	Good
8	Daoud	CEO Office	Advisor	25 – 29	M	5 - 10	Good
9	Saida		Analytics Consultant	35 – 39	F	> 10	Excellent
10	Jamal	Public Relations	Executive Spokesperson	35 – 39	M	5 - 10	Excellent
11	Tarek	Maintenance	Inspector	30 – 34	M	5 - 10	Good
12	Fadil	Human Resources	Manager	≥ 40	M	> 10	Good
13	Salim		Director	35 – 39	M	> 10	Excellent
14	Farida	Educational Institutes	Trainer-Assessor	25 – 29	F	5 - 10	Good
15	Ghazi	Project Management	Manager	35 – 39	M	> 10	Excellent

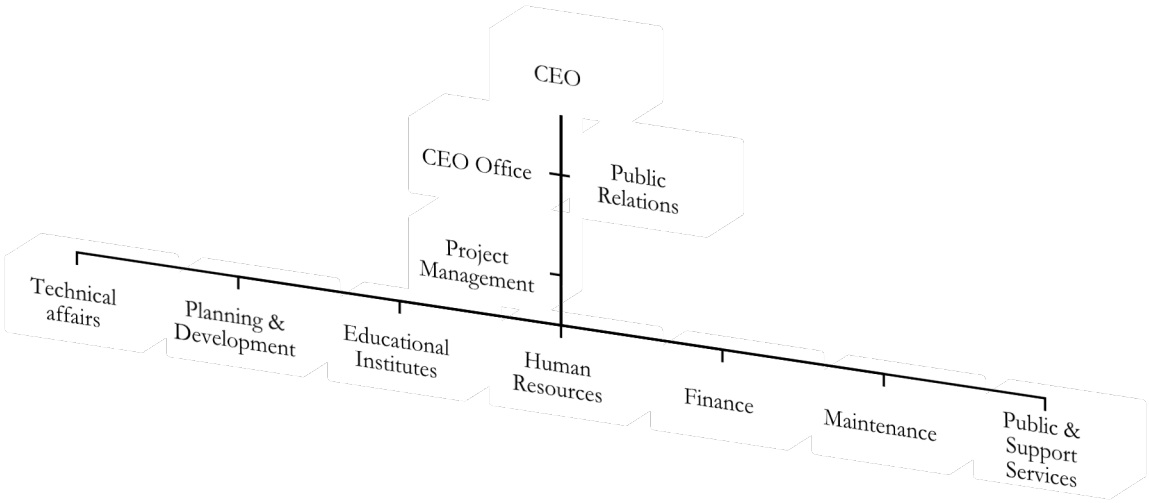
Table 2 – Information Security policy documents

Policy Code	Description
AU12013	Highlights appropriate and inappropriate uses of Information Technology resources and services in the Agency.
IS12013	Details the Agency's Information Security guidelines and recommended security controls.
IU2013	Outlines the appropriate and inappropriate uses of the Agency's internet services namely email and internet browsing activities.
ISG	Summarises the Agency's Information Security policy and guidelines.

Table 3 - Refined themes and final themes: illustrative data

Perceived impact of information security awareness	
ISA as duty of care	"We have an independent information security division and I have noticed that there is an interest, care and seriousness, and such seriousness must be reflected on the information security awareness of employees" (Omar, Economist)
ISA as a dynamic knowledge process	"For an information security campaign to be effective, it needs an acceptable mechanism that does not negatively impact on work and integrates well with it "(Fadil, Human Resources Manager)
ISA as proactive behaviour	"If there is a continuous flow of information and warnings, people will get used to it and start adopting certain behaviours almost naturally. It becomes an ingrained reminder of how to act, it becomes culture" (Ghazi, Project Manager)
Desired impact of information security awareness	
Actionable knowledge to increase resilience	"For me, I think the cognitive side is very important. That is, the knowledge gained through these initiatives is very rewarding to me. It can reduce the risks that can compromise the Agency's systems. This brings benefits to everyone, also on a personal level" (Masud, Industrial Coordinator)
Focus on measuring security levels	"People should have the required information to avoid the loss of equipment, time and effort and the data that might be leaked or exposed" (Fadil, Human Resources Manager)
High engagement through online learning, simulation and interaction	"Traditional training courses take time from employees, and I do not think that every department will be able to send their employees to attend those... training staff for a long period or having a course for a period of several days is not suitable and there are online alternatives that are more interactive" (Jamal, Executive Spokesperson).
Positioning the information security function for influence	"In many matters, the Agency is trying hard to protect itself, but certainly the risk will always be present because of the actions individuals. Certainly, with more than one type of awareness initiative, the benefits will be greater" (EIT29F5H)
Perceived challenges and enablers of information security awareness	
Organisational citizenship	"The underlying basis of all work here is people's awareness that the strength of the Agency's credibility depends on information security. That is a shared concern" (Umar, Auditing Specialist).
Rejection of punitive action	"If an employee is using his devices in the right way or using the official sites and channels to perform work...he is not doing anything positive or negative. He is merely doing the right thing. Sanctions in this context would be disastrous" (Jamal, Executive Spokesperson)
Expansion of security-threat intelligence	"They [organisational insiders] need more in-depth explanation or even face-to-face interaction. They need to implement practically what they learn or to have a specialist at hand who is able to provide them with answers" (Ghazi, Project Manager)
Knowledge-based self-regulation	"Variety is something required, so an employee does not get bored is exposed to change and new experiences. Renewing content is important so that at every period something different is done" (Tarek, Inspector)

Figure 1 – Organisational structure at the case government Agency



Appendix 1 – Interview guide

QUESTIONS	PURPOSE
Organisational introduction	
1) As a governmental organisation in Saudi Arabia, what has been your experience of information security, from the perspectives of policy, awareness and enforcement? 2) As an organisational insider, how would you describe your experience with information security policy and awareness interventions? For instance, have you encountered any information security issues, positive or negative experiences, or do you have practical insights you could tell me more about that relate to your role?	To obtain background information on personal role and experience within the organisation
Landscape	
3) In the current context, organisations are implementing information security awareness programs that include a set of activities such as security awareness training. In your view, what is the real purpose of information security awareness, and how is it possible to deliver on its objectives?	To explore the wider contextual influences of information security awareness interventions
Information security behaviour	
4) Based on you experience of working with and managing people in the Agency, what type of activities or interventions would you say contribute in a most effective way towards improving individual information security behaviour? Prompts: previous information security knowledge; attitudes; values 5) What role specifically do you think belongs to senior management in terms of developing a culture that promotes stronger information security awareness. On the other hand, what do you think might hinder the impact of information security awareness interventions?	To explore the factors that influence information security awareness
Information security awareness interventions	
6) Can you take me through the range of information awareness activities that are set in place at the Agency, especially those that involve training, campaigns, especially designed materials, simulations or other? 7) Looking back in more detail at the activities you have just talked me through, which in your view are more effective and which could be improved and how?	To identify perceived strengths and weaknesses of information security awareness interventions
Close	
8) Are there any other comments/observations that you would like to make regarding the role of information security awareness in the context of governmental organisations?	
Participants profile - Age - Gender - Years of experience in the government sector - Department - Current job position - Computer skills (below average, good, excellent)	