Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2012 Proceedings

European Conference on Information Systems (ECIS)

5-15-2012

IMPLEMENTATION CHALLENGES FOR INFORMATION SECURITY AWARENESS INITIATIVES IN E-GOVERNMENT

Ramzi El-Haddadeh
Brunel University

Aggeliki Tsohou
Brunel University

Maria Karyda
University of the Aegean

IMPLEMENTATION CHALLENGES FOR INFORMATION SECURITY AWARENESS INITIATIVES IN E-GOVERNMENT

El-Haddadeh, Ramzi, Brunel Business School, Brunel University, Kingston Lane, Uxbridge, UB8 3PH, UK, Ramzi.El-Haddadeh@brunel.ac.uk

Tsohou, Aggeliki, Brunel Business School, Brunel University, Kingston Lane, Uxbridge, UB8 3PH, UK, Aggeliki.Tsohou@brunel.ac.uk

Karyda, Maria, Department of Information & Communication Systems Engineering, University of the Aegean, Karlovassi, 83200, Greece, mka@aegean.gr

Abstract

With the widespread adoption of electronic government services, there has been a need to ensure a seamless flow of information across public sector organizations, while at the same time, maintaining confidentiality, integrity and availability. Governments have put in place various initiatives and programs including information security awareness to provide the needed understanding on how public sector employees can maintain security and privacy. Nonetheless, the implementation of such initiatives often faces a number of challenges that impede further take-up of e-government services. This paper aims to provide a better understanding of the challenges contributing towards the success of information security awareness initiatives implementation in the context of e-government. Political, organizational, social as well as technological challenges have been utilized in a conceptual framework to signify such challenges in e-government projects. An empirical case study conducted in a public sector organization in Greece was exploited in this research to reflect on these challenges. While, the results from this empirical study confirm the role of the identified challenges for the implementation of security awareness programs in e-government, it has been noticed that awareness programmers often pursue different targets of preserving security and privacy, which sometimes results in adding more complexity to the organization.

Keywords: Information Security, E-government, Awareness, Implementation Challenges

1 Introduction

The introduction of electronic government (e-government) in the public sector has created an environment in which public sector organisations around the globe realised the importance of utilising their services to be more efficient, transparent, available and citizen oriented (Affisco and Soliman, 2006). The growth and implementation of e-government services depend on marketing and awareness (Reffat, 2003; Navarra and Conford, 2003). There has been always a need for programmes, initiatives as well as campaigns to promote e-government to achieve better participation among various stakeholders for a successful implementation (Weerakkody and Choudrie, 2005; West, 2004). These campaigns would motivate and raise awareness of e-government initiatives including information security. For a successful e-government implementation, there is need to ensure a seamless flow of information across public sector organisations, and at the same time, preserve its confidentiality, integrity and availability. In this respect, information security and privacy have been identified as a challenge for e-government adoption (Ebrahim and Irani, 2005). There has been some little emphasis on the non-technical issues of information security management in e-government (Wang, 2009). A number of studies have identified the lack of security awareness and training, business-orientation, allocated resources, alignment of security strategy with business strategy as the main challenges that can have a considerable impact on the management of information security in e-government (Wang, 2009; Stephen and Rodger, 2006). In this context, information security awareness has been highlighted

as one of the main challenges towards the success of e-government information security implementation (Weerakkody and Choudrie, 2005; Reffat, 2003). The 2010 Ernst &Young security survey (Ernst &Young, 2010) concludes, *"Many current security training and awareness programs are not working as well as they could be"*. Similar findings are provided by researchers who state that not enough attention has been given to the development of theoretical and methodological means for the understanding and management awareness activities (Puhakainen and Siponen, 2010). Recent surveys (CSI, 2009) also indicate that a great part of security losses have their roots on non-malicious, merely careless behaviour of insiders, and that security awareness plays a critical role in formulating a strategic view of information security. Nonetheless, increased security awareness activities are reported at (Ernst &Young, 2011) which states that nearly 70% have run employee awareness programs. The aforementioned indicates that there has been little research on understanding the challenges affecting the implementation of information security awareness initiatives for e-government. The aim of this study is to provide a better understanding of these challenges and how they can contribute towards the success of security awareness initiatives in the context of e-government. Section two provides some background on information security in e-government and information security awareness. This is followed by developing the relevant conceptual framework in section three. Section four highlights the methodological approach used in this study. Analysis and discussion of the empirical case study are included in section five underlining the implications of this research, before ending with some concluding remarks in section six.

2 Background

2.1 Electronic government and information security

The increasing demand for e-government services has raised some concerns on how the management of information security can be successfully utilised (Dhillon and Backhouse, 2001; Dhillon and Torkzadeh, 2006; von Solms, 1999). Rezgui and Marks (2008) have pointed out that maintaining confidentiality, availability and integrity of information is rather more important than the information itself. In this respect, it is imperative to retain information systems security policies and procedures in the delivery of e-government services (Dhillon and Backhouse, 2001). As a result, various information system security standards such as ISO/IEC 27002:2005, Payment Card Industry (PCI), Data Security Standard (DSS), Control Objectives for Information and related Technology (COBIT) and Information Technology Infrastructure Library (ITIL) have been introduced helping private and public sector organisations in their implementation of information systems security policies and procedures (Dhillon, 2007). Interestingly, there has been little research on identifying information systems security implementation challenges in e-government. Studies on e-government information security have offered a number of rich and valuable insights on organisational issues including e-governance, businesses, standardisation, technical infrastructure and usability (Hernon and Calvert, 2005; Tassabehji et al. 2007). It is also, vital, however, to ensure the security of information systems in e-government services taking into considerations threats, vulnerabilities and risk that can exist for any e-government services offered to citizens (Dhillon and Backhouse, 2001). Under these circumstances, significant measures are needed to provide an adequate security level to the organisation's information system. Wilford (2004) argues that researchers in the field of e-government consider security and privacy as one of the key challenges for the implementation of an e-government system. A number of studies have highlighted that data security, accessibility and perceived confidentiality significantly influence individuals' adoption of e-government services (Jaeger, 2003; Lee and Rao, 2003). Moreover, Heeks and Davies (1999:32) specify; *"Senior public officials - both managers and politicians often lack IT skills and even IT awareness"*. In this context, e-government officials must consider training and education as one of the most imperative factors influencing the success of e-government implementation (Read and Kleiner, 1996). Finally, and on a defining note, scholars like Kwon and Zmud (1987) and Anderson and Young (1999) argue that there is a positive relationship between training and implementation success.

2.2 Defining Information Security Awareness

Information security awareness is an inseparable element of a security management scheme (ISO/IEC 27001, 2005). Although security literature acknowledges the necessity of developing security awareness, surprisingly a commonly accepted definition of security awareness is missing. Based on the various approaches, security awareness can be described as a continuous effort of raising stakeholders' attention towards information security and its importance, stimulating security-oriented behaviors (Peltier, 2005; ENISA, 2008, Hansche, 2001; Maeyer, 2007), and ideally inducing stakeholders' compliance to security policies and guidelines (Siponen, 2000).Typically security awareness can be defined via its difference from security training and education and via the changes that targets. Hence despite the different views or perceptions of security awareness it can be concluded from the various definitions that a) security awareness is the first step or the basis of a security learning continuum (NIST, 2003; Hansche, 2001; Peltier, 2005; Katsikas, 2000) and b) security awareness targets changes within an organization (Hansche, 2001; Maeyer, 2007; Cone et al., 2007; Peltier, 2005; Power and Forte, 2006). During the security learning continuum awareness aims at attracting the attention of all IS stakeholders to the importance of information security and their security obligations, training aims at building knowledge and developing the relevant skills and competencies, and education targets security expertise (NIST, 2003; Hansche, 2001; Peltier, 2005; Katsikas, 2000). Security awareness changes vary including changes at end-user's actions, attitudes, work routine and habits (Hansche, 2001; Maeyer, 2007), information security consciousness (Cone et al., 2007), understanding of personal security role and responsibilities (Peltier, 2005), and organizational culture (Power and Forte, 2006).

Although many researchers have explored the intended information security awareness outcomes, literature lacks studies on the managerial aspects of security awareness implementation. Awareness management issues, within the broader security management context, appear because several changes accompany the realization of security awareness initiatives in organizations. These refer to changes required for the awareness program to be implemented or changes that are brought into light due to the awareness activities. In summary, awareness intended and implied changes are not only limited to the individual level, but also expand to the organizational and technical levels.

3 Challenges Influencing Information Security Awareness for e-Government

A close examination of e-government and information security in the literature reveals that, although researchers have highlighted the various factors influencing the implementation of information security awareness initiatives for e-government, these factors can be classified under the four main themes of organisational, technological, political and social. Therefore, in order to better understand the influence of these themes on information security awareness initiatives in e-government implementation, the relevant literature has been examined in detail to identify what challenges can be classified under each of the themes.

Political theme

Information security awareness is considered as an organizational process, since the latter is widely defined as "ways by which organizations accomplish goals". Under the political perspective, the way that politics within the public agency affect the implementation of security awareness is discussed. As a starting point of any security awareness effort Power and Trope (2007) identify the support of top management, as decision makers are the ones who set the example and act as a role model for all staff members. The majority of researchers and surveys (Okenyi and Owens, 2007; Maeyer, 2007; Hansche, 2001; ENISA, 2008) also acknowledge top management support as a fundamental requirement for establishing a successful awareness program. In e-government literature, researchers have pointed out the importance of top management to fully understand the strategic objectives of e-government and the associated benefits (Weerakkody and Dhillon, 2009). By doing so, the

involvement and support of the government's top management would enable them to implement the e-government related projects with more confidence (ibid). For e-government implementation projects, financial issues and support are considered to be one of the main challenges for the development of successful e-government in which funding comes from government where political influence plays a significant role (Eyob, 2004). As a result, the required resources to design and implement a security awareness program depend heavily on top management commitment. Hansche (2001) tackles the assurance of financial resources as one of the main prohibits for an effective security awareness program. Budgetary concerns are also raised by Casmir and Yngstrom (2005) who connect awareness expenses with the overall reluctance for security expenses and the ability of the organization to financially support the protection of its information. Security surveys also repeatedly highlight that the budget allocated to awareness activities is inadequate and limited with regard to its critical role and importance (CSI, 2008; 2009). However, security experts find difficulties in convincing top managers to fund awareness programs, especially because it is difficult to measure their return of investment (Yngström and Björck, 1999; Okenyi and Owens, 2007). This is in line with the general problem to convince top management to invest on information security issue. As Kotulic and Clark (2004) mention, historically threats and vulnerabilities have not been considered until after a security breach had occurred. Moreover, as any other organization project, security awareness should be proposed in terms of a coherent project plan.

Social theme

The social perspective examines how social interactions within an organization influence the implementation of security awareness initiatives. Ethics and personal values are recorded as a significant influence on the success of a security awareness effort. Leach (2003) states that users' personal values and standards of conduct are a critical success factor for awareness, because it is important that the individual's values and the company's values are in line otherwise conflicts arise. Siponen (2000) also argues that morals and ethics critically affect users' motivation to act in a security conscious way. An additional influence is derived from the interpretation of security messages from their recipients. Security experts typically use a technical language when referring to the information system's operations and components, threats and vulnerabilities. NIST (1998) refers to this as the 'security alphabet'. However, the security messages should be communicated to the target audience in a language that they understand. Security technical terms are difficult to understand by end-users and managers (Peltier, 2005). Desman (2003) further supports this argument; if awareness designers want people to understand them they should speak their language. Moreover, security messages need not only to be understandable, but also to be created with a marketing point of view. In other words, security awareness should "sell" information security to stakeholders, using attractive and persuasive messages (Peltier, 2005). Desman (2003) proposes that security messages should be developed with a sense of humour and Hansche (2001) highlights that the tone of security messages will affect their attractiveness. By definition security awareness targets a broad range of audience and recipients of awareness messages. However, security awareness should not be planned and designed without the participation of different IS stakeholders. It is fundamental for security awareness efforts to engage not only the IT department, but staff members from all departments (Power and Forte, 2006). Stimulating security consciousness of top management is also highlighted as high priority, despite the fact that awareness efforts are commonly believed to target end-users primarily. Engaging all the organizational hierarchy is also recorded by Maeyer (2007), who states that in the cases that top management initiates awareness programs, but line managers are not engaged, then the employees most probably will not change their behaviours. Leach (2003) also supports this argument, arguing that employees are likely to adopt the practices of people around them. Kritzinger and Smith (2008) propose the involvement of IS stakeholders from all authority levels; board, executive management, middle management, technical, security management, end-users. Finally, Albrechtsen (2007) points out that the more effective approach to enhance security awareness is to involve users in the overall security effort.

Organizational theme

Information security awareness is situated within a security management scheme and a broader organizational context; hence, it is affected by organization characteristics. Power and Forte (2006) demonstrate that organizational structure is a significant factor in implementing a successful security awareness program. In their empirical setting, the various awareness design and implementation roles and responsibilities to realize the awareness initiative were allocated to the existing security roles of the organizational hierarchy; namely the Communications Officer, the Intelligence Officer and the Chief Security Officer. Organizational structure is also identified as an affecting element by ENISA (2008), since organizational roles are interpreted to awareness roles regarding design and implementation; e.g. top management approves the program's funding. In the context of e-government projects, the roles are perceived as the needed ICT activities which require time and appropriate frameworks to support the implementation pocess (Marchewka, 2006; Ebrahim and Irani, 2005).

Similarly, business and security objectives are closely related to security awareness implementation. As Spurling (1995) highlights, it is critical for the success of an awareness initiative that the organization has a clear direction towards which all security policies, practices, and procedures are founded; a security vision. In his empirical case, he exemplifies how this factor was important for designing a customized awareness program in line with the established security infrastructure and the minimization of problems from the existence of too many authentication accounts for each user. Alignment with the business goals and general security vision is also highlighted by Peltier (2005). Finally, ENISA (2008) records the importance of aligning security awareness with business strategy.

Spurling (1995) and Okenyi and Owens (2007) identify the existence of a security policy in the organization as an important influence to security awareness. Having a security policy that reflects the security philosophy and vision of the organization, is crucial for designing a security awareness program that is truly customized to the organization's needs. A security policy documents the high level security goals and objectives, which act as requirements for the awareness program in order to design awareness actions that propose work practices in line with the other organizational policies and procedures. Moreover, the existence of an organizational security policy assures that similar treatment is enforced for similarly risky users' behaviours; hence awareness efforts can stimulate consistent attitudes. Security Awareness Index Report (2002) concludes that the lack of adequate policy practices is a leading cause of poor security awareness levels among organizations. Another important influence relates to the management of the awareness effort. Among the reasons why security awareness programs fail to deliver a lasting value is the lack of managing awareness programs as formal projects with formal objectives, milestones and resources (Maeyer, 2007). Hansche (2001) also argues that in order to achieve top management commitment and ensure financial support for such an effort a project plan that will describe the objectives, cost estimates, time schedules and deliverables planned is essential.

Technological theme

Information security standards act as a fundamental input for building a security awareness program. Peltier (2005) identifies security standards as a way of ensuring that programs and systems work in harmony. Standards represent a commonly agreed and practically derived knowledge, which act as a cost-saving process that supports the efficient running of organizations. Technology standards are important requirements for e-government implementations. Relevant literature highlights a number of challenges that affect establishing a collaborative environment between government agencies and its respective employees (Fedorowicz et al., 2009; Joia, 2007). It is common for different government agencies to have different, incompatible architectures that may not maintain seamless functionality, leading to implementation difficulties.

Protecting information security often creates conflicts with the established work practices. Information security procedures sometimes may be opposite to efficiency, usability and functionally making users unwilling to follow them and adopt awareness propositions. Albrechtsen (2007) points out that one of the main obstacles that users face in order to adopt security-oriented attitudes is the conflict between

functionality and security. Security countermeasures and awareness actions should pay attention to prevent as less as possible creating difficulties for work functionality and efficiency. Moreover, many awareness actions or exercises require some kind of technical support in order to be implemented. Dodge et al (2007) present an exercise to evaluate users' awareness on phishing attacks. In order the exercise to become feasible, a supporting architecture should be established; mainly a mail server and a database server responsible for the management of phishing mails and responses. Similarly, Cone et al. (2007) promote security awareness via a video game. The building blocks of the suggested game consist of a simulation engine, a domain-specific scenario definition language, a scenario development tool, and a video enhanced encyclopaedia.

Summing up the aforementioned theoretical arguments which were identified within information security awareness and e-government literature, a conceptual taxonomy is developed to map the key factors influencing the implementation of information security awareness initiatives in e-government under the four main themes; political, social organisational, and technological, as presented in Table 1.

Table 1 Implementation challenges of information security awareness initiatives in e-government

Theme	Factor	Description	Reference
Political Theme	Top management commitment to security awareness	Support provided by top management throughout the security awareness initiative, including them acting as a role model for all stakeholders.	Power and Trope (2007), Okenyi and Owens (2007), Maeyer (2007), Hansche (2001), ENISA (2008)
	Resources allocated to awareness	Financial, human and other resources required for awareness implementation. Literature refers that resources allocated to awareness are, so far, inadequate.	Hansche (2001), Casmir and Yngstrom (2005), CSI (2008, 2009)
	Awareness return of investment	Security awareness return of investment is difficult to quantify. This becomes an obstacle in attaining management approval.	Yngström and Björck (1999), Okenyi and Owens (2007)
Social Theme	Stakeholders' ethics and personal values	Stakeholders' personal values and codes of conduct strongly affect their behaviour and their motivation to follow promoted behaviours.	Leach (2003), Siponen (2000)
	Language used for promoting information security	The language used in communicating information security should be simple and understandable by all IS stakeholders.	Peltier (2005), Desman (2003)
	Marketing-oriented security messages	Drawing attention towards security requires a marketing approach, including humour and attractive messages.	Peltier (2005), Desman (2003), Hansche (2001)
	Involvement of all stakeholders	The engagement of staff members from all departments and authority levels is required.	Power and Forte (2006), Maeyer (2007), Leach (2003), Kritzinger and Smith (2008), Albrechtsen (2007)
Organizational Theme	Organizational structure	The responsibilities for implementing in-house security awareness project are commonly allocated to existing roles in the organization structure.	Power and Forte (2006), ENISA (2008)
	Awareness project management	Raising security awareness is a project that requires a systematic implementation approach. Formal objectives, milestones and resources should be identified.	Maeyer (2007), Hansche (2001)
	Business and security vision	A clear security vision that directs all security policies and procedures ultimately enhances security awareness implementation.	Spurling (1995), Peltier (2005), ENISA (2008)

	Security policy	The existence of a security policy enhances the design of an awareness program that is dedicated to specific security needs and the promotion of security within the organization.	Spurling (1995), Okenyi and Owens (2007), Security Awareness Index Report (2002)
Technological Theme	Information security and awareness standards	Standards' guidelines derive from best practices. Guidance on security awareness implementation will help to avoid common mistakes and solve common problems.	Peltier (2005)
	Conflict between security and IS functionality	Security countermeasures selection and implementation in a way that produces minimum functionality conflicts facilitates security awareness.	Albrechtsen (2007)
	Technical support for awareness implementation	Security awareness actions or exercises many times require technical support in order to be implemented.	Dodge et al. (2007), Cone et al. (2007)

4 Research design and Case Study Presentation

The purpose of this study is to explore the implementation challenges that are faced when an information security awareness initiative (programs, campaigns, etc.) is realized in the public sector. To do so, the relevant literature on e-government and information security was analysed to identify the internal and external challenges of information security awareness implementation in organizations as reported by researchers and practitioners. In order to explore the recognized challenges in the public sector identified in the conceptual framework, a case study was selected as an idiographic research. In idiographic research, as proposed by Franz and Robey (1984), the researchers examine in depth a single entity or a particular event in an attempt to better understand a phenomenon in its context. On the opposite, a nomothetic research strategy aims at producing generalizable results and laws.

The empirical investigation involves a public sector organization in Greece (referred to in this paper as Information Systems Government Agency–ISGA). ISGA is responsible for developing, implementing, functioning and monitoring large-scale information systems for the Greek public sector; these include information systems for supporting taxation, customs services, public sector payroll and retirement pension etc. Information security requirements are quite high as the organization processes personal and sensitive citizens' information, such as payroll and medical data, allowances, information under the tax secrecy, citizens' accusations etc. The organization adopts a hierarchical structure that includes top management, executive management, senior management and directors levels. Semi-structured interviews with all management members (top managers, executive managers, senior managers, directors and administrators, fourteen individuals in total) were used for the collection of empirical data.

The effort began when the authors agreed with one of the ISGA directors for the importance of a security awareness effort for the organization. Following a long-lasting effort the researchers contacted and agreed with top management the collaborative development of the awareness program. The security awareness program was developed following the guidelines published by ENISA (2008). Series of meetings between the security experts and all executive managers, senior managers, directors, and several employees (selected by their directors) have followed for designing the awareness program. The security awareness design was completed ten months later and was presented to top management. The awareness plan included thirteen proposed awareness actions such as periodic distribution of information on privacy and on personal data protection via email, distribution of leaflets and posters for promoting information privacy and physical security. The validation and initiation of the awareness program emerged to be a long-lasting process. The awareness plan was validated after 5 months and the actual implementation began three months later and became a continuous effort.

5 Empirical findings and discussion

Through the interviews conducted, the authors have identified a number of different issues that followed the implementation and diffusion of information security awareness programmes for e-government in ISGA. The findings are analyzed according to the framework of organisational, social, political and technology themes proposed earlier in section 3.

Political theme

Top management support dominates as an influential factor to information security awareness implementation (Power and Trope, 2007; Okenyi and Owens, 2007; Maeyer, 2007; Hansche, 2001; ENISA, 2008). The case study findings significantly support the role of top management commitment. First, the awareness initiative failed to be approved when the security experts agreed with the ISGA's director on the initiation of the awareness program. Only after top management was formally engaged to the effort the security awareness project has initiated. Second, it was necessary to attain a formal validation by both top managers through the whole process; i.e. for defining awareness objective and goals, target groups, communication plan, overall awareness plan. Third, top management commitment acted as a role model for the importance of security; as top manager declared "*the implementation of the security day event will depict the actual commitment and direction of ISPO towards information security*".

The resources allocated to awareness have been identified as an implementation barrier (Hansche, 2001; Casmir and Yngstrom, 2005; CSI, 2008, 2009), as well as the difficult to allocate resources due to uncertain return on investment (Okenyi and Owens, 2007). Budgetary concerns were raised from the beginning of the project when the top manager requested "*A formal document or letter describing the human, financial and time resources that will be needed*". Despite the fact that top management has fully undertaken the implementation coordination and communication for the awareness actions, ultimately adequate financial resources were not allocated which prevented the implementation of specific awareness actions; e.g. actions that required printing facilities. As a justification of the resources allocation the top manager argued that awareness will be the starting point of "*regarding information security horizontally and more strategically*". Moreover, he requested to the security experts to develop a "*press release that will demonstrate the organization's effort*". The case study findings also support legislation as a significant influence to the awareness implementation. Data protection and tax secrecy laws were driving the overall security management efforts in the organization. In the context of information security awareness programmes in e-government, public administrators need to implement new strategies, which will require new rules and regulations to re-shape its services in order to facilitate public sector transformation (Doherty and King, 2001).

Social theme

The language used in the security messages should be simple and the communication style should adopt a marketing perspective (Peltier, 2005; Hansche, 2001; Desman, 2003). Following ENISA (2008) guidelines the target stakeholders were separated into different audience groups and the security promotion messages were designed accordingly to their role and technical knowledge using various and attractive communication channels, such as presentations, flyers, posters, artefacts. Satisfying the two requirements stimulated the conversation during the security workshop at which the majority of audience groups participated. The engagement of staff members from all departments and authority levels is required (Power and Forte, 2006; Maeyer, 2007; Leach, 2003; Kritzinger and Smith, 2008; Albrechtsen, 2007). Top management has undertaken all coordination activities, during awareness design, including organizing meeting and inviting the responsible individuals. The involved roles included most high hierarchy roles, such as senior managers and directors, and only few employees. However, audience during the security event expressed their desire to be more involved in related activities. They also acknowledged that "*they did not have enough information to judge the importance or the content of the security event, which led to reduced participation*". Finally they asked more similar events to be organized. Thus, transformation will then influence the

implementation of new rules, procedures and organisational processes as in information security awareness programmes that relate to as well as shape social behaviours of public sector employees (Liang et al., 2007; Teo et al., 2003).

Organizational theme

The role of organizational structure for awareness implementation is mainly connected to the allocation of responsibilities for the awareness design and implementation (Power and Forte, 2006; ENISA, 2008). According to the case study findings this can be more highlighted when the Security Officer role is missing. Top management considered the establishment of an information security department in the organization as a prerequisite to launch the security awareness program. Especially for public administration agencies this influence becomes even more evident because organizational changes are quite bureaucratic and strongly connected to power distribution and authorities. In our case study the request for a security department was turned down by the politically assigned top manager and the Ministry of authority, on the grounds of changes to organizational structure. The project halted for several months and ultimately begun without the presence of official information security role. Following the guidelines of ENISA (2008) the security experts have developed a formal awareness plan, as also suggested in the literature (Maeyer, 2007; Hansche, 2001), which was validated by the management. The awareness plan incorporated a proposal for new organizational roles to support the long-term awareness implementation, but their implementation has not progressed. Hence, the sustainability of several awareness actions was threatened due to the lack of official security authorities. For example, the creation of a security and privacy newsletter could not be allocated to any of the existing organizational roles, resulting in confusion for the project's implementation. A clear business vision (Spurling, 1995; Peltier, 2005; ENISA, 2008) and an established security policy (Spurling, 1995; Okenyi and Owens, 2007; Security Awareness Index Report, 2002) facilitate awareness implementation. The absence of a clear security vision and the presence of multiple security policies for the different information systems confused security awareness design. "*There is no high-level security policy. Only information system specific security policies exist*", was stated by developers, employees and directors. As top manager stated it was a priority to "*regard information security horizontally and more strategically, in contrast to the isolated efforts that have already been made in the organization, and they view the security awareness initiative as a first attempt to this aim*".

Technological theme

Technical support has a significant role on awareness implementation (Dodge et al., 2007; Cone et al., 2007). With the exception of leaflets, posters and security artefacts, in our case study the proposed awareness actions involved different kinds of technical development or integration, such as creation of mailing lists and automatic updates, development of security and privacy wiki or intranet, supporting security forums and periodic newsletter. As a technical support executive reported regarding security communication "*there is no feedback mechanism at place enabling users to provide their concerns and opinions*". The organization faced many difficulties to realize the technological changes which resulted in the partial implementation of the awareness plan. Finally, the case study findings confirm that the existence of security standards facilitates awareness implementation, as reported by Peltier (2005). The role of ENISA (2008) awareness guidelines was dominant for both convincing top management for the security experts eligibility and for the actual project's coordination and planning. In this respect, the appropriate use of ICT standards and systems integration including information security and awareness standards can provide the required support towards the successful implementation of e-government projects. In the literature, several authors such as Irani et al., (2008) identified IT standards as a major factor during the implementation and integration of various technologies in an e-government context.

6 Conclusion

When reflecting on the literature on e-government information security awareness programmes implementation presented in this study, the authors argue that there are challenges imposing pressure on public sector's organisational structure and processes. As a result, this may have a major impact on their success or failure towards implementing change. This study has contributed to the body of knowledge by providing a better understanding of information security awareness initiatives implementation in e-government. The empirical study in this paper offered the conceptualisation of the challenges influencing information security awareness initiatives implementation in the context of e-government. Through this study, the authors have attempted to highlight some of the key factors that can enable the success of e-government information security awareness initiatives implementation. While the e-government information security literature showed there is a lack of prior research that explores the political, organisational, social and technological challenges, the conceptual model presented in this paper offered the required platform for outlining these challenges.

As outlined from the empirical findings; political, organisational, social and technological challenges have a considerable as much as significant impact on the implementation of information security awareness initiatives in e-government projects. Top management commitment, resources and return of investment have been outlined as the main organisational challenges facing the implementation of information security awareness initiatives. Stakeholders' ethics and personal values, use of promotion language, marketing messages and involvement of relevant stakeholders have been identified as the social challenges. Further, organisational challenges included structure, project management, business and security vision and security policy. Finally, the technological challenges emphasized on information security and awareness standards, conflict between securities and IS functionality and technical support for awareness implementation. Moreover, it is often the case that pursuing different targets of preserving security and privacy are conflicting with each other, thus creating a complex organizational issue. Future research efforts are needed to conduct further studies in a number of different public sector organisations to explore the relevance of the issues identified in this paper and to identify any further issues. In addition, the authors point out to the need to investigate other stakeholders' needs in relation to adequacy of information security awareness programmes for e-government adoption, which can help to provide further understanding between e-government implementation and use.

7 References

Affisco, J. F. & Soliman, K. S. (2006) E-government: a strategic operations management framework for service delivery. Business Process Management Journal, 12, 13-21.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & Security, 26 (4), 276-289

Anderson, S. W. & Young, S. M. (1999) The impact of contextual and process factors on the evaluation of activity-based costing systems. Accounting, Organizations and Society, 24, 525-559.

Casmir, R. and Yngstrom, L. (2005). Towards a dynamic and adaptive information security awareness approach. In Proceedings of the IFIP TC11 WG11.8 Fourth World Conference on Information Security

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen T. D. (2007). A video game for cyber security training and awareness. Computers & Security, 26 (1), 63-72.

CSI (2009), "Computer crime and security survey 2009", Computer Security Institute. Available at: http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey09_Executive-Summary.pdf (Accessed at 30.11.2011)

Desman B. M. (2003), The Ten Commandments of Information Security Awareness Training. Information Systems Security, 11(6), 39-44

Dhillon, G. and Backhouse, J. (2001), Current directions in IS security research: towards socio-organizational perspectives, Information Systems Journal, 11(2), 127 – 153.

Dhillon, G. and Torkzadeh. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16, 293-314.
Dodge, R. C., Carver, C., & Ferguson A. J. (2007). Phishing for user security awareness. Computers & Security, 26 (1), 73-80
Doherty, N. F. & King, M. (2005) "From Technical to Socio-Technical Change: Tackling The Human and Organizational Aspects of Systems Development Projects, European Journal of Information Systems, 14(1), 1-5.
Ebrahim, Z. & Irani, Z. (2005) E-government adoption: architecture and barriers. Business Process Management Journal, 11, 589-611.
ENISA (2008). A new Users' Guide: How to Raise Information Security Awareness. European Network and Information Security Agency.
Ernst & Young (2010), "12th annual global information security survey: Outpacing change", Available at: http://www.ey.hu/TW/en/Issues/Managing-risk/Information-security-and-privacy (accessed 30.11.2011)
Ernst & Young (2011), "Into the cloud, out of the fog", Available at: *http://www.ey.com/GL/en/Services/Advisory/IT-Risk-and-Assurance/Information-security*, (accessed 30.11.2011)
Eyob, E. (2004) E-government: breaking the frontiers of inefficiencies in the public sector. Electronic Government, an International Journal, 1, 107-114.
Franz, C.R. & Robey, D. (1984), "An Investigation of User-Led System Design: Rational and Political Perspectives." *Communication of the ACM*, 27, 1202-1209.
Hansche, S. (2001), Designing a Security Awareness Program: Part I. Information Systems Security, 9(6), 14-23.
Heeks, R. & Davies, A. (1999) Different approaches to information age reform. Reinventing government in the information age: international practice in IT-enabled public sector reform, 22-43.
Hernon, P. and Calvert, P. (2005), E-service quality in libraries: Exploring its features and dimensions, Library & Information Science Research 27, pp. 377–404.
Irani, Z., Love, P. E. D. & Jones, S. (2008) Learning lessons from evaluating eGovernment: Reflective case experiences that support transformational government, Journal of strategic information systems, 17(2), 155-164.
ISO/IEC 27001 (2005), Information technology - Security techniques – Information security management systems – requirements. International Standards Association
Jaeger, P. T. (2003) The endless wire: e-government as global phenomenon. Government Information Quarterly, 20, 323-331.
Katsikas, S. (2000). Health care management and information systems security: Awareness, training or education? International Journal of Medical Informatics, 60(2), 129–135.
Kotulic, A.G. & Clark, J.G. (2004), Why there aren't more information security research studies? Information & Management, 41 (5), pp.597-607.
Kritzinger E. and Smith E. (2008), Information security management: An information security retrieval and awareness model for industry. Computers & Security, 27(5-6), 224-231.
Kwon, T. H. & Zmud, R. W. (1987) Unifying the fragmented models of information systems implementation. Wiley Series In Information Systems, 227-251.
Leach, J. (2003). Improving user security behavior. Computers & Security, 22(8), pp. 685-692
Lee, J. K. & Rao, H. R. (2003) Risk of Terrorism, Trust in Government, and e-Government Services: An Exploratory Study of Citizens' Intention to use e-Government Services in a Turbulent Environment.
Liang, H., Saraf, N., Hu, Q. & Xue, Y. (2007) Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. Management Information Systems Quarterly, 31, 59.
Maeyer, D. D. (2007). Setting up an Effective Information Security Awareness Programme. In: ISSE/SECURE 2007 Securing Electronic Business Processes Highlights of the Information Security Solutions Europe/SECURE 2007 Conference (part 1), Vieweg, 49-58

NIST (1998). Information technology security training requirements: A role- and performance-based model. In M. Wilson (ed.), NIST Special Publication 800–16. Gaithersburg, MD: National Institute of Standards and Technology.
NIST (2003). Building an information technology security awareness and training program. In M. Wilson (ed.), NIST Special Publication 800–50. Gaithersburg, MD: National Institute of Standards and Technology.
Navarra, D. D. & Cornford, T. (2003) A Policy making view of E-Government Innovations In Public governance. Proceedings of The Ninth Americas Conference On Information Systems. Tampa, Florida.
Okenyi, P. O., and Owens, T. J. (2007), On the Anatomy of Human Hacking. Information Systems Security, 16 (6), 302-314.
Peltier, T. R. (2005). Implementing an Information Security Awareness Program. Information Systems Security, 14 (2), 37- 48.
Power M. and Trope R. (2007), Developing a Culture of Privacy: A Case Study. IEEE Security & Privacy 5(6): 58-60.
Power, R., & Forte, D. (2006), Case Study: a bold new approach to awareness and education, and how it met an ignoble fate. Computer Fraud & Security, 2006 (5), pp. 7-10.
Puhakainen P. and Siponen T.M. (2010), "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study". MIS Quarterly, 34(4), 757-778.
Read, C. W. & Kleiner, B. H. (1996) Which training methods are effective? Management Development Review, 9, 24-29.
Reffat, R. (2003) Developing A Successful E-Government. School Of Architecture, Design Science And Planning. University Of Sydney, Australia.
Rezgui, Y. and Marks, A. (2008), Information security awareness in higher education: An exploratory study, Computers and Security, 27(7-8), 241-253.
Security Awareness Index Report. (2002). The state of security awareness among organizations worldwide. ITToolBox and Pentasafe, 2002. From Web Site: http://security.ittoolbox.com/pub/
AM101502a.pdf [accessed at: 10–09–2011].
Siponen M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8 (1),. 31-41. Education (WISE4), May 2005, Moscow, Russia
Spurling, P. (1995), Promoting security awareness and commitment, Information Management & Computer Security, Vol. 3 No. 2, 20-6.
Stephen S. and Rodger J., (2006). Determining Key Factors in E-Government Information System Security, Information Systems Management, 23 (2), 23-32
Tassabehji, R., Elliman, T. and Mellor, J. (2007) Generating Citizen Trust in E-Government Security: Challenging Perceptions, International Journal of Cases on Electronic Commerce, 3(3)
Teo, H. H., Wei, K. K. & Benbasat, I. (2003) Predicting intention to adopt interorganizational linkages: An institutional perspective. MIS Quarterly, 27(1) 19-49.
von Solms, B. (1999). Information security management: why standards are important. Information Management & Computer Security, 7 (1), 50-57.
Wang, Jin-fu (2009). E-government Security Management: Key Factors and Countermeasure, In: Proceeding of Fifth International Conference on Information Assurance and Security IAS' 09
Weerakkody, V. & Choudrie, J. (2005) Exploring E-Government in the UK: Challenges, Issues and Complexities. Journal Of Information Science and Technology, 2, 26-44.
Weerakkody, V. & Dhillon, G. (2009) Moving from E-Government to T-Government: A Study of Process Reengineering. Handbook of Research on Strategies for Local E-government Adoption and Implementation: Comparative Studies, 1.
West, D. (2004) E-Government and the Transformation Of Service Delivery And Citizen Attitudes. . Public Administration Review, 64, 15-27.
Yngström, L., & Björck, F. (1999). The Value and Assessment of Information Security Education and Training. In: Proceedings of the IFIP TC11 WG11.8 First World Conference on Information Security Education (WISE1), Stockholm, pp. 271-292.