Addressing Organisational, Individual and Technological Aspects and Challenges in Information Security Management: Applying a framework for a case study

Ioanna Topa
University of the Aegean
itopa@aegean.gr

Maria Karyda
University of the Aegean
mka@aegean.gr

Abstract

This study investigates information security management challenges in a large organisation. The aim of this study is to apply the Technological-Organisational-Individual (TOI) Framework in this organisation to determine to what extent current security management practices are informed by findings of relevant literature and standards on information security incorporated in the framework. The TOI framework is used to map factors influencing security behavior to current practices applied by the organisation and to analyse them. Conclusions suggest that some factors that play a critical role in information security management are not adequately covered. This study also aims to provide recommendations to security managers on how to address these factors to implement security management practices that can improve ISP compliance, and inform literature on any additional security management practices. Further, this study includes insights into how organisations may exploit key strengths in applying information security management to achieve good security behaviour among their employees and take an adaptive approach to changing conditions, such as teleworking.

Keywords: Information security management practices, security behaviour aspects, technological-organisational-individual framework

1. Introduction

Security threats have increased dramatically over the last few years and organisations need to be protected from a variety of sophisticated threats, including phishing, ransomware, spyware, etc. (Varonis, 2021). This can be achieved by employing security countermeasures and practices outlined in information security management standards such as in ISO/IEC 27001(ISO/IEC 270001, 2013). However, research studies have posited that security countermeasures alone are not sufficient, and the security behaviour of employees must be considered for security management practices to be effective (Bulgurcu et al., 2010; Herath & Rao, 2009a). Teleworking, which has grown due to the COVID-19 pandemic, has made human error the biggest cybersecurity challenge according to Chief Information Security Managers (CISOs)(Security, 2020), with 95% of cybersecurity breaches being caused by human error (Varonis, 2021). Therefore, it is vital to identify factors that influence employees to form a security behavior. Current literature on information security behaviour provides a wealth of theoretical information, which can be very useful to security managers (Cram et al., 2017). Nevertheless, given the highly complex nature of this field and the inherent difficulties for security managers in understanding highly theoretical studies (D'Arcy & Lowry, 2019; Sommestad et al., 2017; Siponen et al., 2022; Topa, 2019), previous research (Topa & Karyda, 2019) has suggested that security managers can benefit greatly from a more practical aid to guide them. An analysis of critical factors affecting security management according to related literature is presented in the form of a Technological-Organisational-Individual (TOI) Framework in (Topa, 2019). This framework encompasses security behaviour determinants influencing employees towards complying with information security policies (ISPs) and using security tools, along with the implications of these factors in practice, as identified in relevant literature (Cram et al., 2017; Bulgurcu et al., 2010; D'Arcy et al., 2009; Dinev & Hu, 2007; Herath & Rao, 2009a; Herath & Rao, 2009b; Hu et al., 2012; Ifinedo, 2012; Ifinedo, 2014; Johnston et al., 2003; Kolkowska, 2011; Pahnila et al., 2007; Safa et al., 2016; Siponen et al., 2014; Son, 2011; Vance et al., 2012; D'Arcy & Herath, 2011; D'Arcy & Greene, 2014; Connolly et al., 2015). This framework (Topa, 2019) informs security managers on all factors that need to be addressed, including issues such as habits, culture and values, which are not currently outlined in

URI: https://hdl.handle.net/10125/102687
978-0-9981331-6-4

widely used security management best practices and standards, such as the ISO/IEC 27000 series.

The main aim of this study is to apply the TOI Framework in practice and identify whether current security management practices are informed by the TOI framework aspects. The authors perform a gap analysis by mapping the TOI framework aspects to current security management practices followed by the organisation in question. Analysis shows that important aspects are not adequately addressed. Recommendations are provided to guide security managers on how to implement these aspects and design security management practices to enhance ISP compliance, based on security management guidelines outlined in (Topa & Karyda, 2019). Furthermore, insights are gained on additional security management practices that are followed by this organisation.

The structure of the paper is as follows: Section 2 presents an introduction to the TOI framework and its application. Section 3 outlines the research design. Section 4 presents the results of the study, which are then analysed in Section 5. This includes an analysis of the main security management practices followed by the Organisation and the degree to which they are successfully applied (based on the TOI framework). Section 6 provides recommendations for enhanced security management in this Organisation. This is followed by discussion of the findings in Section 7 and conclusions in Section 8.

2. Theoretical Background: TOI Framework explained

The TOI framework (Topa & Karyda, 2019) derives from a comprehensive literature review of factors influencing security behaviour and a review of the ISO Standards (namely ISO 27001, 27002, 27003 and 27005). This framework provides a comprehensive overview of the most significant factors involved in information security behaviour, classified according to three essential categories, namely, Technological, Organisational and Individual (Topa, 2019). Other frameworks cover some of these categories, but not all three of them, e.g. the Technological-Organisational-Environmental (TOE) framework does not address individual factors and the Technological-Personal-Environmental (TPE) framework does not cover organisation-related factors (Jiang et al., 2010).

The aim of the TOI framework is to aid security managers by providing them with a clear and practical means of applying current knowledge on security management practices. This framework is applied to the Organisation in this study as a means of determining how well the security management practices of the Organisation correspond to the relevant, generally accepted ISO standards and to findings from current literature.

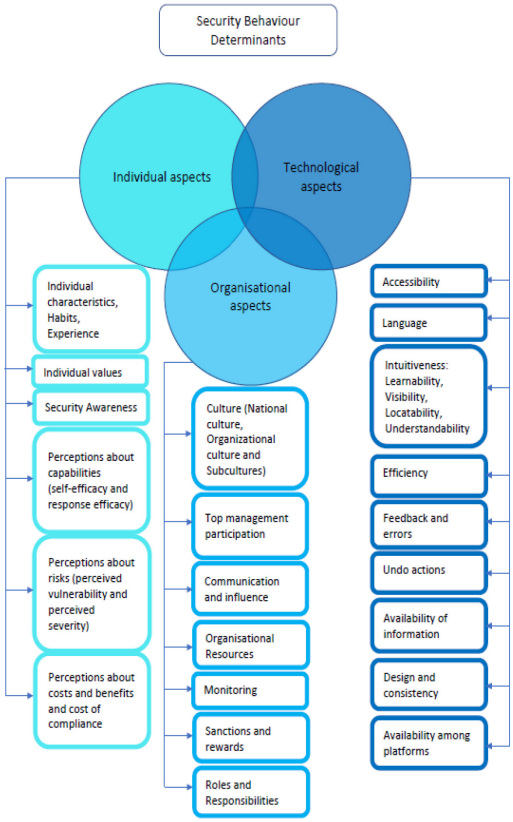

Figure 1: Technological-Organisational-Individual Framework (Topa, 2019).

2.1 Organisational aspects

According to literature, one significant aspect of security behaviour is *culture*, which includes *national culture, organisational culture* and *subcultures* (Connolly, 2015). In terms of *organisational culture*, flat management encourages employees to give feedback on security issues and comply with ISPs (Connolly, 2015). When employee feedback is considered during ISP creation, this leads to ISPs that are not cumbersome (Kirlappos et al., 2015).

Top management participation influences employees' security behaviour (Hu et al., 2012). More importantly, top managements' actions should be visible to employees to convey the message that ISP compliance is vital and that since top management complies with ISPs, all other employees are expected to follow their example (Hu et al., 2012).

Communication among employees is a factor motivating them to comply with ISPs (Ifinedo, 2014).

For example, through formal or informal meetings employees exchange views about security issues. One significant aspect of communication is *knowledge sharing* (Safa et al., 2016), where employees pass their security knowledge on to colleagues. An important role is also played by *social influence*, namely the way in which employees' security behaviour is influenced by others' actions and beliefs (Herath & Rao, 2009a).

Organisational resources including help from experts, time to get used to new ISPS, training and seminars can all motivate users to comply with ISPs (Pahnila et al., 2007). Furthermore, the quality of the ISPs with regard to easily understandable *language* and up-to-date content is also significant in determining security behaviour (Pahnila et al., 2007).

According to literature, a further important aspect is the existence and visibility of *monitoring controls*, which influences employees' security behaviour (Herath & Rao, 2009b).

Likewise, *sanctions and rewards* are security behaviour determinants (Bulgurcu et al., 2010), though it is noteworthy that literature gives contradictory findings, with cases where sanctions or rewards have no impact on employee security behaviour (Siponen et al., 2014; Pahnila et al., 2007; Son, 2011).

2.2 Individual aspects

One significant group of *individual* aspects comprises characteristics such as *age, gender, habits* and *experience*. Literature findings suggest a correlation between age and compliance with ISPs, with older employees being more compliant (D'Arcy & Greene, 2014), as well as between the two genders**,** with female employees showing higher compliance rates (Ifinedo, 2014). Additionally, there is evidence that greater compliance can be achieved through habitualising certain security behaviours (Son, 2011; Topa & Karyda, 2016). Similarly, an individual with IS experience will find it easier to comply with ISPs (Safa et al., 2016).

Concerning individual *values*, research points to the importance of ISPs being regarded as appropriate and legitimate (Son, 2011), as well as the importance of individuals' values being in tune with those of their organisation (Son, 2011).

As findings from current literature indicate, there are several types of individual awareness that impact security behaviour and which therefore need to be addressed by security managers. In addition to *ISP awareness* (Bulgurcu et al., 2010), these include *technology awareness* (Dinev & Hu, 2007), *general knowledge of information security* (Bulgurcu et al., 2010), *awareness of monitoring mechanisms* and *awareness of SETA programs* (D'Arcy et al., 2009).

Finally, there are a number of aspects related to individual *perceptions*. These may concern the individual's *confidence* in their own ability to deal with security tasks, often referred to as self-efficacy (Herath & Rao, 2009a). There is reference to the individuals' perceptions about the *effectiveness of their actions* if they comply with the ISPs and also to the *effectiveness of ISPs*; this factor is identified as response efficacy (Herath & Rao, 2009a; Ifinedo, 2014). There are also individual perceptions regarding *security risks* to their organisation and their *severity* (Siponen et al., 2014) or how individuals perceive the possible *benefit* or *cost of compliance* with ISPs, mainly in terms of time, effort and convenience (Bulgurcu et al., 2010).

2.3 Technological aspects

A*ccessibility* of security tools (Seffah et al., 2006) relates to security tools being accessible to people with disabilities.

Literature findings suggest that the *language* used in security tools has to be clear and plain, easy to understand, and without too many technical terms. This is particularly important for non-IT employees (Topa & Karyda, 2018).

A significant technological aspect of security tools that covers a broad range of closely related features is *intuitiveness*. One feature is *learnability*, namely that tools need to be easy for users to learn how to use (Topa & Karyda, 2018). Tools also need to have security settings that are easily locatable (*locatability*) and visible (visibility) (Furnell, 2010; Johnston et al., 2003; Topa & Karyda, 2018). For example**,** users need to be able to find the security settings easily without spending too much time and also there should be security indicators (namely graphs, pictures or illustrations) to show them what is happening inside the system in terms of security. Additionally, they should naturally guide the users, helping them understand how to use them (*understandability*) (Topa & Karyda, 2018; Whitten & Tygar, 2005). To maximise their usability and in turn achieve better ISP compliance, security tools should be *efficient* and not create additional time delays or inconvenience to users (Topa & Karyda, 2018; Whitten & Tygar, 2005).

A further usability characteristic that can improve security tools' effectiveness is the provision of *feedback* to users (Murayama, 2012). Users want to receive information regarding *errors* as well as being able to *undo their actions* (Topa & Karyda, 2018). Furthermore, other usability characteristics are

availability among platforms, *minimalistic design* and *availability of help and suppor*t (Johnston et al., 2003).

3. Research Design

Research was carried out over a three-month period in one branch of the IT Department of a large public sector organisation, situated in a European capital, which also operates in other European countries. Research was carried out two years prior to the COVID-19 pandemic. This is a public institution that deals with legislative measures and budget programming. However, for reasons of confidentiality, more information about this organisation cannot be revealed. This is a large public-sector organisation and therefore a significant budget is invested yearly for information security. Because of the size and nature of this Organisation, which deals with sensitive and confidential information, information security is of paramount importance and therefore it is in the Organisation's interests to be vigilant in terms of information security and to address new security risks e.g. teleworking risks. For this reason, security management of this Organisation was open to recommendations based on academic research with a view to improving their security management practices.

The first objective was to identify the information security management practices that were in place (e.g. Awareness, Top Management, Communication, etc.) and map these against the TOI framework aspects, to assess them. Through analysis of current practices it would then be possible to identify any shortcomings in terms of security management, and to propose potential improvements to further enhance security management practices based on the TOI framework (Topa & Karyda, 2019). A further objective was to identify any new, interesting or effective practices followed by the Organisation.

The data for the analysis was gathered in three ways: interviews with employees and management, passive observation of employees' and management's security behaviour, and detailed analysis of documentation related to information security practices and information security policies (ISPs). Interviews were conducted with the Organisation's IT security personnel and members of the management team in the IT security department to gain a comprehensive idea of the current security management practices that are followed. Approximately 50% of interviewees were employed in administrative positions and 50% were technical staff. Questions (both open and closed) concerned information security and covered areas such as employees' beliefs and perceptions about information security, security awareness, information security practices followed by employees, support and help with information security issues and the existence of sanctions and rewards regarding information security behaviour. The focus was on determining how well their security behaviour corresponded to the aspects of the TOI framework. There were interviews with 30 people (5 managers). Ethical considerations were taken into account to ensure that information included in this study promotes educational purposes, ensures confidentiality of sensitive information and preserves anonymity of the participants.

Additional information was gained through passive observation of employees and managers in their day-to-day security tasks as well as observation of the Organisation's environment. These observations were conducted during the course of employees' daily work, without any comments or interruptions. The focus of the observations was two-fold: identifying organisational aspects of information security such as the workplace environment and identifying individual behaviours relevant to information security. More details cannot be revealed for reasons of confidentiality. This study also included analysis of ISP documentation such as policies regarding Information Security, User Access Management, Individual Equipment, Acceptable Use, etc. and processes (e.g. Remote Access Connection) and the process of creating new ISPs was observed.

4. Findings

The TOI framework was applied to the specific Organisation to identify the information security management practices in relation to the technological, organisational and technological aspects. Findings are presented below.

TOI aspects	Findings
Organisational aspects	
Culture	Multi-cultural, hence no significant national behaviour trends
Top management participation	Security behaviour followed (passwords, guest accounts)
Communication and influence	• Daily meetings, high degree of communication • More experienced colleagues regularly consulted • Support by IT Helpdesk
Organisational Resources	• Formal ISP documentation • A guide to security threats • A website on the intranet • Posters & Cards • An ISP for teleworking.

Monitoring	Maintaining logging and monitoring tools
Sanctions and rewards	No sanctions and rewards
Roles and Responsibilities	Clearly assigned roles and responsibilities, e.g. Local Information Security Officer (LISO)
Individual aspects	
Habits	Cards depicting good security behaviour
Individual values	Individual values match the organisational values, e.g. mutual respect, fairness, equality
Security Awareness	• Info sessions seminars • Security-related conferences
Perceptions about capabilities	Employees show sense of self confidence in complying with the ISPs
Perceptions about risks	No major concerns about the likelihood of IT security threats (research was carried out before regular teleworking)
Perceptions about costs and benefits/ cost of compliance	Ask for employees' feedback to minimise cost of compliance
Technological aspects	
Accessibility	Software is selected to be accessible by people with disabilities
Language	Antivirus tool from leading vendor and language easy to understand
Intuitiveness	Intuitive antivirus
Feedback	Feedback was noticeable, e.g. status feedback

Table 1: Findings from the Applicability of the TOI Framework to the organization.

5. Analysis: Security management practices in the Organisation

Findings show that the Organisation generally addresses a variety of factors that are described in the TOI framework regarding organisational, individual and technological aspects. Below is a description of the Organisation's security management practices which correspond to aspects of the TOI framework. These derive from the authors' assessment based on their experience, employees' observations and interviews.

5.1 Practices supporting Organisational aspects

5.1.1 Culture. Employees are of multiple nationalities. Given that it is a multi-cultural working environment, no significant behaviour trends originating from employees' national culture were observed. Rather, there is a strong emphasis on *organisational culture* through practices that promote organisational goals and values (in particular equality, mutual respect, fairness, communication and collaboration). This was made clear by the statement of one of the interviewees, in a managerial position *"we treat all colleagues equally, irrespective of their type of job or seniority"*.

5.1.2 Top management participation. *Top management* follows security practices, by securing their computers with passwords and creating guest accounts when access to their computer is needed by other colleagues, etc.

5.1.3 Communication and influence. All employees of the Organisation participate in formal and informal meetings on a daily basis to discuss work issues and make decisions. This is facilitated by a general organisational culture encouraging *communication* between employees. It is common practice for colleagues to visit each other in their offices or communicate through phone calls or video teleconferencing. Communication plays a pivotal role in the day-to-day functioning of the Organisation, which strongly promotes collaboration and also ensures that employees discuss work issues with superiors and co-workers. In this way, employees are encouraged to share their knowledge on all work-related issues, including security practices. It is also customary for employees to consult more experienced colleagues, while those with greater experience readily offer advice and support. This openness and willingness to help on the part of more experienced employees ensures that those less knowledgeable about information security have access to the necessary support and do not feel intimidated by a lack of expertise in dealing with IS practices, leading to *self-efficacy* (Herath & Rao, 2009a).

Furthermore, it was observed that employees ask for IT experts' help at the helpdesk on any IT or security-related issues, in particular those with less IT experience. *Resource availability*, e.g. help from experts, is a factor which influences employees to comply with ISPs (Herath & Rao, 2009a).

5.1.4 Organisational Resources. This Organisation provides a facilitating environment in terms of *resources* (security documents, posters, cards, training, etc.), which is a practice that motivates users to comply with ISPs (Herath & Rao, 2009a). All employees have access to information regarding information security practices. There is formal documentation for raising employees' security *awareness* and informing them of the appropriate

security behaviour. On the intranet there is an online guide to security threats, such as phishing, etc., and a website about IT and security issues. Finally, a newsletter is sent by email on a regular basis.

In various visible locations, such as at the building's entrance, posters inform staff about how to deal with security issues such as phishing. On various stands located in different areas employees can also pick up cards which promote IS security, using illustrated messages to highlight the difference between good and bad security practices (e.g. a picture of a desk where the desktop computer and mobile devices such as smartphones and tablets are in clear view, unlocked and unattended, in sharp contrast to the adjacent image of a desk where everything is organised, the desktop computer is locked and there are no mobile devices visible). The caption "Better safe than sorry" below clearly warns users not to leave their devices unattended and unlocked.

The Organisation recognises the need for a shift from the traditional workplace to a more flexible teleworking scheme and has developed an ISP for teleworking, written in easily understandable *language* without many technical terms. Through this ISP employees can be adequately informed of the security threats and risks involved in teleworking and form the appropriate security behaviour.

5.1.5 Roles and Responsibilities. The Organisation has clearly assigned *roles and responsibilities* in terms of information security with the IT security department being responsible for ensuring information system security. In every department, e.g. Finance, Communication etc., there is a person for admin operations. This person also acts as a Local information Security Officer. More specifically, he/she is the point of contact for security incidents that might take place and responsible for reporting them to the security department. This person serves as a "security champion" (Ifinedo, 2012).

5.2 Practices supporting Individual aspects

5.2.1 Habits. Cards depicting the need for ISP compliance, e.g. the clean desk policy, are located all around the premises, thus employees are constantly but discreetly reminded of the need to form the appropriate security behaviour as well as the underlying consequences of not being security-conscious (the simple use of the caption). This message seems to be conveyed successfully as an interviewee stated *"this card illustrates an example of a good security behaviour in an easy and understandable way. By having this card on my desk, I am constantly reminded of the actions I need to take".*

5.2.2 Security Awareness. Special 'info sessions', seminars to inform employees about security threats and vulnerabilities, take place on a quarterly basis. During these seminars employees are informed of security issues and tools to raise their security *awareness*. Employees of the IT security department participate in security-related conferences.

5.2.3 Perceptions about the cost of compliance. In order to minimise the *cost of compliance*, security managers of this Organisation improve ISPs by making them user-friendly (e.g. use of clear *language*) and asking for employees' feedback and views.

5.3 Practices supporting Technological Aspects

5.3.1 Usability - Accessibility and Intuitiveness. The antivirus tool is centrally configured for all computers, without the need for employee involvement. Furthermore, since the Antivirus tool was from a leading vendor, *language* was easy to understand and *feedback* was easy to notice (e.g. the tool's status or about updates).

In terms of *accessibility*, the Organisation selects software suitable for people with disabilities. Employees with disabilities pre-test software to determine whether it is usable. This indicates the Organisation's interest in tool usability and in ensuring that employees with disabilities can access the appropriate software.

6. Recommendations for the enhancement of security management practices

While the Organisation has implemented certain security management practices, some factors that are mentioned in the TOI framework are not adequately implemented in practice. This section provides recommendations based on practical guidelines by Topa & Karyda (2019) to improve ISP compliance.

6.1 Establishing a Facilitating Organisational Environment

The Organisation provides resources to promote information security. However, a few employees may not respond appropriately to the information supplied, e.g. some employees might not pick up one of the cards. One suggestion would be to send the relevant

material to users individually, e.g. by email or post it on the intranet where everyone has access.

6.2 Engaging Management's Involvement and Compliance

The Organisation has a clearly hierarchical organisational structure, being organised into Departments, with every department having its own Director. Every department consists of Units supervised by the appropriate management personnel. Top management plays a significant role, as employees conform to the directions of their superiors and to the guidelines of the Director.

As in any large organisation, *top management* is not so visible, and it is difficult for employees to see their involvement in security-related issues. As this Organisation is one where employees appear to follow the advice, instructions and behaviour of superiors, this would suggest that top management has a highly influential role. Given this existing advantage, it is recommended that security managers exploit this influence more fully by actively engaging management towards complying with ISPs, e.g. by encrypting confidential data, sending emails about information security and participating in security-related meetings and trainings. Consequently, top management will set employees a more visible example of good security behaviour.

6.3 Promoting security knowledge through awareness and training programs

Training material is available on the intranet and training sessions take place for raising employees' awareness about security issues. While useful, it is important for security managers to check that all employees both assimilate the material and know how to deal with such security issues. Thus, hands-on training and regular checks such as online questionnaires or self-assessment tests are recommended to verify that employees have assimilated the information security knowledge.

Additionally, special leave could be given to employees who participate in security-related trainings, thus acting as an incentive.

Aside from training, another important aspect that literature suggests is the need for security managers to consider employees' confidence in following ISPs (Siponen et al., 2014; Herath & Rao, 2009a; Vance et al., 2012; Ifinedo, 2012; Siponen et al., 2014). Although this Organisation places emphasis on employees taking responsibility for their own security actions, while at the same time strongly encouraging communication and support among colleagues and between employees and superiors, some employees may lack confidence in their ability to deal with certain security tasks. Thus, it is recommended that the Organisation optimise opportunities for employees to gain the relevant skills and knowledge as well as assess their level of competence through self-assessment tests, simulations of information security attacks, simulations of phishing campaigns, etc.

6.4 Designing and Implementing ISPs, Security Practices and Controls

6.4.1 Assigning Roles and Responsibilities. The Organisation has assigned roles in every department, all of which have their own IT Department and the IT administrator is also assigned the role of Local Information Security Officer. In some cases, however, employees do not seem fully aware of this specific role. Security managers can rectify this by regularly communicating to employees the existence of certain IT security positions and responsibilities. This can be achieved during training, seminars and meetings organised by the Local Information Security Officers of each Department.

6.4.2 Applying Sanctions and Rewards. Regarding *sanctions*, the Organisation's security management practices do not include specific sanctions for employees who fail to comply with ISPs. Given that sanctions have mixed results in terms of effectiveness (Topa & Karyda, 2019), and the fact that they might conflict with this Organisation's values of equality, collaboration and communication, sanctions might be ineffective in this case. In more competitive organisations, however, sanctions such as warnings or even dismissal are regarded as an effective means of ensuring ISP compliance (D'Arcy et al., 2009). In this particular Organisation one "neutral" measure would be to send fake phishing emails to all staff**,** with mandatory security training imposed on any employee who clicks on the fake link.

Currently the Organisation does not offer specific *rewards* for employee compliance, perhaps because current security management standards like ISO 27001 do not stipulate specific types of sanctions or rewards. However, given the benefits of a reward system (Bulgurcu et al., 2010), when an employee identifies a security breach such as a phishing fraud and duly reports it to security personnel, he/she could receive a "thank you" email that would also be seen by his/her superiors. This would reflect the Organisation's emphasis on positive behaviours, highlight the value the Organisation attaches to

employees and act as an incentive to enhance information security behaviour.

6.4.3 Applying Monitoring Controls. To enhance compliance, except for log inspection and monitoring it is recommended that Local Information Security Officers perform informal walk-in checks to see whether employees are following ISPs; checking, for example, whether employees write their passwords on post-its and put them in visible places, or whether they properly lock their laptops or keep them in a secure place when unattended.

6.4.4 Accommodating Individual Characteristics, Values and Habits. While literature suggests that security managers could employ targeted training methods for specific individual characteristics e.g. age or gender (D'Arcy & Greene, 2014; Ifinedo, 2014), this does not seem an appropriate practice for this Organisation, which promotes equality. However, when communicating ISPs, security managers could exploit the Organisation's egalitarian philosophy by informing all stakeholders that ISPs should be followed by everyone, without exception, from top management to ordinary employees.

Current practices, such as security-related posters or cards on stands promote ISP compliance out of habit. In addition to this, security managers could allocate time in employees' daily work schedule to carry out security tasks to further foster the practice of following them out of habit (Topa & Karyda, 2019).

6.4.5 Selecting and Implementing Appropriate Security Controls. The Organisation's organisational culture, which, among others, promotes the values of equality, extends to installing software that is accessible to all employees, including those with disabilities. The practice of disabled staff testing software to ensure its compatibility with their needs could be extended to security tools.

6.5 Leveraging Social Influence and Promoting Security Communication

Since employees of this Organisation communicate closely on a daily basis, they are influenced by their colleagues' actions and expectations (Herath & Rao, 2009a). Security managers could exploit employees' social influence and interaction more fully by encouraging Local Information Security Officers to communicate more regularly with employees and inform them about information security issues (e.g. security incidents).

TOI Focus areas	Practical Recommendations
Establishing a Facilitating Org. environment	Communication of material to employees. Checking assimilation of knowledge.
Engaging Management's Involvement/Compliance	More visible top management security actions.
Promotion of security knowledge through awareness and training	Hands-on training, self-assessment tests, simulations of IS attacks/phishing campaigns.
Assigning Roles and Responsibilities	Raising awareness about the role of Local Information Security Officers.
Applying Sanctions and Rewards	Mandatory training to employees who respond to fake phishing emails. Reward mechanism for good security behaviour.
Applying Monitoring Controls and Mechanisms	Adoption of informal walk-in checks.
Accommodating Individual Characteristics, Values and Habits	Emphasis on ISPs being followed by everyone, from top management to employees Allocation of specific time for daily security tasks.
Selecting and Implementing Appropriate Security Controls	Accessibility of security tools for disabled people.

Table 2: Practical Recommendations.

7. Discussion

This Organisation applies certain security management practices which can enrich current literature on information systems security management. Specifically, the use of cards and posters depicting the contrast between good and bad security behaviour is a useful practice motivating employees to form the appropriate security behaviour out of habit. Further, special focus is given to the implementation of a teleworking ISP to make employees aware of the security threats and how to minimise them. Currently ISP compliance studies focus mainly on employees working in traditional workplaces, while only a few investigate employees' security behaviour for teleworkers (D'Arcy & Herath, 2011). According to (D'Arcy & Herath, 2011) deterrent effects deriving from sanctions and monitoring are weaker for teleworkers. As teleworking is rapidly becoming popular within organisations, due to the recent pandemic, scholar research should further explore how

this change in the working environment impacts employee security behavior.

Research has posited that sanctions and rewards have mixed results (Siponen et al., 2022; Topa & Karyda, 2019). While this Organisation currently applies no specific rewards or sanctions, this study proposes the implementation of sanctions and rewards appropriate to the Organisation's values and culture.

This study involves a large, institutional Organisation with a considerable budget invested in IT security and whose nature, size and resources enable it to address many factors that influence ISP compliance. Findings may well differ in smaller private companies, or those of a different nature, which suggests there is a need for further research which would broaden the scope of the TOI framework's application. The study highlights that when applying security management practices, security managers should not adopt a 'one-size-fits-all' approach by simply applying technological controls and practices as stated in best practices and standards. Security managers can make use of the TOI framework by understanding the context of their organisation first and then by mapping the factors of the framework to the current practices to identify key strengths and design a strategy for implementing security management practices which exploit these key strengths and promote the cultivation of a security culture.

Due to the size of the Organisation as well as work and time constraints, it was not possible to extend the research to all staff members in all departments, or to study certain technological factors in detail.

8. Conclusions

While a number of widely accepted security management practices are implemented by the Organisation, certain aspects in the TOI framework are not adequately addressed and therefore recommendations are provided on how to implement these to promote ISP compliance. These recommendations include checking employee assimilation of security knowledge, promotion of employees' confidence in complying with ISPs, making top management's involvement more visible, raising awareness of the role of the LISO, implementing mild sanctions in the form of mandatory training, applying rewards, adopting informal walk-in checks, promoting the message that ISPs must be followed by all employees, allocating specific times for daily security tasks and extending the Organisation's policy of selecting software accessible to disabled staff to include security tools.

A number of practical insights were gained including the use of cards to cultivate appropriate security behaviour out of habit as well as the effective creation of an organisational culture based on values of equality and communication. The design of a teleworking policy written in clear and simple language shows an organisation adapting to the changes of modern teleworking trends and addressing the human aspect. Although this study was conducted prior to the COVID-19 pandemic, it highlights the need for security managers to be flexible to the changing conditions brought about by new technologies, pandemics and crises. To be prepared, security managers can use the TOI framework as a roadmap making them aware of all factors influencing security behaviour. Furthermore, they can exploit this study as an example of the TOI framework being applied in practice and gain insights into how to design their security management practices to promote improved ISP compliance as well as cultivating an information security culture. As future work, it would be useful to follow up on whether the recommendations are implemented and determine any resulting differences in security behaviour. Given its relevance to current times, it would be beneficial to extend the application of the TOI framework to organisations of different sizes and types.

Competing Interests: The authors declare no competing interests. This text expresses the personal opinion of the author (I.T.) and not that of the European Court of Auditors.

9. References

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), pp. 523-548.

Connolly, L., Lang, M., & Tygar, J. D. (2015, May). Investigation of employee security behaviour: A grounded theory approach. In IFIP International Information Security and Privacy Conference (pp. 283-296). Springer, Cham

Cram, W. A., Proudfoot, J. G., & D'arcy, J. (2017). Organizational information security policies: a review and research framework. European Journal of Information Systems, 26(6), 605-641.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems, 20(6), 643-658.

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Information Systems Journal, 29(1), 43-69.

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, 20(1), pp. 79-98.

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. Journal of the Association for Inf. Systems, 8(7), p. 386.

Furnell, S. (2010). Usability versus complexity–striking the balance in end-user security. Network Security, 2010(12), 13-17.

Herath, T., & Rao, H. R. (2009a). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.

Herath, T. and Rao, H.R. (2009b).“Encouraging information security behaviors in organisations: role of penalties, pressures and perceived effectiveness”, Decision Support Systems, 47(2), 154-165.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012).Managing employee compliance with information security policies:the critical role of top management and organisational culture.Decision Sciences,43(4),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,31(1), pp.83-95.

Ifinedo, P. (2014). Information systems security policycompliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, 51(1), 69-79

ISO/IEC 27001. (2013), ISO/IEC 27001:2013. Information technology-Security techniques-ISM systems-Requirements.

Jiang, Y., Chen, D., & Lai, F. (2010). Technological-personal-environmental (TPE) framework: A conceptual model for technology acceptance at the individual level. JITIM, 19(3), 5

Johnston, J., Eloff, J. H., & Labuschagne, L. (2003). Security and human computer interfaces, 2003. Comput. Secur. 22, 675–684.

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). " Shadow security" as a tool for the learning organization. Acm Sigcas Computers and Society, 45(1), 29-37.

Kolkowska, E. (2011). Security subcultures in an organisation-exploring value conflicts. ECIS.

Murayama, Y., Fujihara, Y., Saito, Y., & Nishioka, D. (2012). Usability issues in security. In International Workshop on Security Protocols (pp. 161-171).

Nielsen, J. (1994). Usability engineering. Morgan Kaufmann.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07) (pp. 156b-156b). IEEE.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in Organisations. Computers & Security, 56, pp. 70-82.

Security (2020). Human error poses cybersecurity challenges for 80% of businesses during the COVID-19 pandemic (Available at: https://www.securitymagazine.com/articles/93885-human-error-poses-cybersecurity-challenges-for-80-of-businesses-during-the-covid-19-pandemic)

Seffah, A., Donyaee, M., Kline, R. B., & Padda, H. K. (2006). Usability measurement and metrics: A consolidated model. Software Quality Journal, 14(2), 159-178.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees’ adherence to information security policies: An exploratory field study. Information & management, 51(2), 217-224.

Siponen, M., Pahnila, S., & Mahmood, A. (2006, November). Factors influencing protection motivation and IS security policy compliance. In 2006 Innovations in Information Technology (pp. 1-5). IEEE.

Siponen, M., Soliman, W., & Vance, A. (2022). Common Misunderstandings of Deterrence Theory in Information Systems Research and Future Research Directions. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 53(1), 25-60.

Sommestad, T., Karlzén, H., & Hallberg, J. (2017). The theory of planned behavior and information security policy compliance. Journal of Computer Information Systems.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees’ motivation to follow IS security policies. Information & Management, 48(7), 296-302.

Topa I, (2019).Analysing IS Behaviour:Technological-Organisational-Individual Framework and Practical Guidelines to Enhance ISP Compliance, PhD Thesis

Topa, I., & Karyda, M. (2018, September). Usability characteristics of security and privacy tools: The user’s perspective. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 231-244). Springer, Cham.

Topa, I., & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. Information & Computer Security.

Topa, I., & Karyda, M. (2016). Analyzing security behaviour determinats for enhancing ISP compliance and security management. In European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS).

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. Information & Management, 49(3-4), 190-198.

Varonis (2021).134 Cybersecurity Statistics and Trends for 2021.(Available:https://www.varonis.com/blog/cybersecurity-statistics)

Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In USENIX Security Symposium (Vol. 348).