For cited: *Afacan, O. (2019). Encouraging Employees on Compliant Behaviours about Information Security Measures in Workplaces. Journal of Current Researches on Social Sciences, 9 (1), 87-102.*

Journal of Current Researches on Social Sciences (JoCReSS)
www.stracademy.org/jocress
ISSN: 2547-9644

Year:2019
Volume: 9
Issue: 1

Research Article/Araştırma Makalesi

Crossref doi: 10.26579/jocress-9.1.6

Encouraging Employees on Compliant Behaviours about Information Security Measures in Workplaces

Onur AFACAN[1]

Keywords
Information security, compliance, cyberscurity, confidentiality, integrity.

Abstract
The development of technology and computer use has become a critical issue with increasing national and international laws, standards and information security in the present day. Attacks on information systems, destruction of information, the possession of third parties are an indication of the size of the risks.
This study is based on answers from department managers who operate in different areas of Istanbul but work on information security. It is the main objective to measure the degree of awareness of users about information security. The work was carried out through the managers and managers of the units, which are mostly operational areas. All of the employees have undergraduate and higher education levels and their average age is 41.
The participants were evaluated by asking questions about the employees' knowledge of information security, how they are aware of the importance of the issue, the applications performed, how the control and follow-up are performed and what applications can be developed.
Information security is a critical issue for all employees, especially managers. Therefore, information security policies should be developed in institutions, these policies should be shared with all employees and information security awareness trainings should be given to the users.

Article History
Received
12 Feb, 2019
Accepted
14 Mar, 2019

1. Introduction

Information Technology has become an integral part of today's businesses. And few businesspeople can afford to be without the specialized computing and security knowledge that enables them to make sound decisions. They need to know the risks an enterprise faces, and the methodologies and technologies that are available to minimize those risks.

This research aims to determine the opinions and observations about the control mechanisms of the enterprises or institutions regarding the protection of information security and the continuity of information security by the employees of enterprise.

Research takes place in a global security company. Therefore, this study guides and advise management on more effective implementations in the firm. It is tried to

[1] Corresponding Author. ORCID: 0000-0003-3294-7381. İstanbul Aydın Üniversitesi, onurafacan@stu.aydin.edu.tr; onurafcn@gmail.com

conduct ''want to'' mechanism instead of ''have to''. Also, having contribution to company's IS operations, making the management understand the reasons of the gaps, increasing awareness about the effects of attitudes and behaviours on IS compliances, providing continuous motivation to comply IS measurements and helping management to conduct more effective IS culture in the organization are the other topics which point the significance of the study.

It is assumed that the individuals participating in the survey responded by expressing their opinions completely without any influence or pressure. Within the scope of the research, managers' views are limited to the qualifications covered by the semi-structured interview form. Besides, interviews were done with only security department.

2. The Concept of Information Security

There are many definitions of information. Information is defined as data recorded, classified, organized, related or interpreted within context to convey meaning (Duffy and Assad, 1980: 13). Another definition is that information is any physical form of representation or surrogate of knowledge or of a particular thought used for communication (Farradane, 1979: 13). It is possible to define information simply as data endowed with relevance and purpose.

Information helps us to reduce uncertainty and make decisions in different situations. In other words, information is used in making decisions and taking actions based on the decisions made. Information has a vital role in each part of life. For the reason that it is not possible to hold all the information, exchange of data between different departments, institutions, people or technologies is needed. Unfortunately, sharing of information increases the risks that an organization faces. Because of this fact, the person who shares information has to take actions to protect it from any internal or external threat.

Security is simply defined as "the state of being protected or safe from harmfreedom from danger" (http://www.merriam-webster.com/dictionary/security).

Information is one of the most important assets that an organization holds. Because of this fact, it has to be protected properly and continuously by the organization. In order to provide the continuity of its operations, an organization should ensure the protection of information against any threats. The threats that an organization can be faced with may be either external or internal. Security is composed of two very important components: physical and electronical. For this reason, information must be protected both physically and electronically.

Information security is simply defined as the preservation of confidentiality, integrity, and availability of information (ISO/IEC 27001 Standard). According to the Committee on National Security Systems (CNSS), information security is the protection of information and its censorious components, including the systems and hardware that use, store, and transfer the information.

In the case of unauthorized access, use or destruction of information or information systems, information security takes place in order to provide protection against any threat that can occur.

2.1. Organizational Information Security Culture

Many efforts have been made within the last decade to explore and address the IS related issues. Researchers (Chang and Ho, 2006; Eloff and Eloff, 2003; Sittig and Singh, 2010) generally agree that IS management encompasses many domains, including managerial, technical, social and organizational aspects that must all be effectively addressed. Similarly, other studies also indicate that IS issues similar to safety and quality are more of social rather than technical issues involving business, organizational, management, and people elements (Dhillon and Backhouse, 2000; Dutta and McCrohan, 2002; Mader and Srinivasan, 2005).

Solms identifies the issue as one of the 10 sins stating as “not realizing that the protection of information is a business issue and not a technical issue” (von Solms and von Solms, 2004: 372). The socio-technical nature of information security is also emphasized by Björck and Siponen (Björck, 2004; Siponen, 2006) and the human dimension to both IS practice and technology design is recognized (Coles-Kemp, 2009: 181). Lampson (2004) and Lacey (2010) support the view that IS management is a people problem, not just a technology problem, as it is people who will implement, manage, and use the IS policy within an organization.

Still, some research in business to manage and define IS indicate more attention is given on a technical and operational level without a formal framework or methodology (Hong et al., 2003). Additional research confirms that IS has been regularly measured as a technological problem with a technological solution (Ruighaver et al., 2007: 56), All these studies focusing on finding technological solutions to prevent vulnerabilities and attacks tend to overlook human and organizational aspects and do not adopt a socio-technical approach which involves human and organizational aspects (Dhillon and Backhouse, 2001: 140).

Having a training culture that brings awareness to issues as well as solid procedures and policies in place before any problem occurs is important. Similarly, user feedback on policies and procedures is essential to improve their effectiveness. Kenneth et al. (2009) state that, when individuals are not motivated to follow procedures and protect information, security fails. Theodorakis (1994) indicate that employees indirectly cause the majority of the problems by violating and neglecting existing organization IS policies.

From a theoretical perspective, information security systems (ISS) have "technical, socio-technical, or social organizational roles." According to the technical view, information security is a technical artifact and the emphasis in regards to security is on technical matters, with social implications in second place if at all exist. (Iivari and Hirschheim, 1996: 553). Technical view where users have no direct responsibility in ISS development measures considers poor technical quality and user resistance as the main causes for IS problems. The socio-technical view, on the other hand, considers both technical and organizational factors equally important and points out the non-existence of an asymmetry between social and technical systems as the source of ISS problems (Iivari and Hirschheim, 1996: 556). Compared to technical view, users in socio-technical view have moderate participation and responsibility related to ISS activities. Finally, the social view stresses the importance and priority of the development of organizational systems

with respect to technical matters, where fulfilling users' preferences have a major impact on the success of the ISS efforts.

As IT is designed and used by humans, human-computer interaction (HCI) is very important and IS solutions that do not consider how users will react to and comply with them are likely to fail. One of the main characteristics of socio-technical studies is its consideration of the interaction between the technology that is constructed and the people who affect and are affected by the technology including the HCI component. The socio-technical view emphasizes human factors in security management. According to this approach, risks are separated as human risks and technical IS risks. Due to the sociological nature, the risk is seen as subjective rather than objective. A variety of theories from different disciplines such as psychology and sociology have been used as a reference for exploration of IS risk management (Appari and Johnson, 2010).

A wide variety of models have been developed under various studies trying to examine the factors in IS. Kankanhalli et al. (Kankanhalli et al., 2003: 141) focus on prevention methods pointing out that deterrent and preventive efforts using control procedures are one way to deal with non-compliance and misuse of systems by employees. Torres et al. (2006) outline some success factors based on current IS literature and security experts' perspectives. Reason (1997) focuses on safety factors that in certain cases prevent incidents such as human errors contributing to IS issues. Ives and Olson, (1984) identify user participation as an important element in IS risk. Fulford and Doherty (2003: 106) summarizes key factors (Siponen, 2000: 31; Von Solms, 1998: 174) contributing to effective IS management as: "the commitment and support from information security management; conducting assessment of potential security risks and threats; the implementation of appropriate controls to minimize risks and threats; and the communication of security issues."

Major factors found to influence IS in organizations are (Waly et al., 2012: 4); lack of awareness, lack of defining roles and responsibility, lack of communication and documentation, lack of reward and sanction systems, lack of reinforcement and practice.

2.2. Organizational Culture

The short-hand, well-known, common, and simplest definition of organizational culture is "the way things are done here" (Bower, 1966; cited by Smit and Dellemijn, 2011: 23). According to Robbins (2001), organizational culture can be considered as the personality of the organization (Robbins, 2001; cited by Da Veiga and Eloff, 2010: 198) and is the social glue that binds the members of the organization together (Kreitner and Kinicki, 1992; cited by Da Veiga and Eloff, 2010: 198).

Organizational culture can be viewed as a combined effort between anthropology (Roethlisberger and Dickson, 1939; cited by Scott et al., 2003: 924) and sociology (Parsons, 1977; cited by Scott et al., 2003: 924), which also contributed to the scientific management techniques of Frederick W. Taylor and his successor Frank B. Gilbreth. These two underlying approaches form the platform for various theories and/or paradigms that study organizations (Burrell and Morgan, 1979;

cited by Scott et al., 2003: 924). Anthropology uses interpretivism to explain culture via a metaphor for an organization, defining organizations as being cultures. Sociology, however, uses functionalism to define culture, as something an organization owns. Pettigrew introduced the term "organizational culture" to literature in an article in "Administrative Science Quarterly" (Pettigrew, 1979: 572) even though Jaques referred to it as "culture of a factory" as early as 1951 (Jaques, 1951; cited by Scott et al., 2003: 924).

Though roles, norms, and values all have been mentioned by Katz and Kahn (1978: 5) in their "The Social Psychology of Organizations", it wasn't until the late 80s when organizational culture according to (cited by Scott et al., 2003: 925) has been defined by various scholars (Davies et al., 2000; Schein, 1988). The definitions include a wide range of social phenomena, such as language, behavior, beliefs, values, norms, assumptions, symbols of status and others. Among all these definitions, Edgar Schein's (Schein, 1985; 1988: 7) definition that utilizes a functionalist view seems to have the most acceptance and usage.

According to Schein, practices, and behaviors, values and beliefs, and underlying assumptions form the three levels of culture. Practices and behaviors, which are hard to measure deal with organizational attributes, and are observed, felt and heard within an organization by individuals. Values and beliefs which deal with goals, ideal norms, standards, and moral principles are measured through survey questionnaires. Underlying assumptions form the essence of the organizational culture

2.3. Information Security Culture

IS culture requires more attention as social and cultural aspects of employee interactions within workplace and technology is an issue as reported by many (Guzman et al., 2008). Research indicates organizational culture and information systems management, in general, are correlated, which includes IS (Smit and Dellemijn, 2011: 31)

The compliance behavior is reported to be influenced by organizational subcultures causing conflicts within departments. Studies indicate for the compliance of IS, security culture plays an important role (Ma et al., 2008). Winkel defined security culture as "the system of collective moral concepts, mindsets and behavior patterns anchored in the self-conception of a social unit and instructing its members in dealing with security threats" (Winkel, 2007: 223). Rotvold indicated security culture provided a positive effect on security compliance (Rotvold, 2008). Chang and Lin (2007), examining the overall influence of organizational culture on the IS management implementations (cited by Bess, 2012) indicated that favorable organizational culture is needed for a suitable and effective IS management implementation, as well as technology and management's support.

Better understanding, developing and managing a proper information security culture inside an organization is not easy to accomplish. Industry researchers and academic scholars (Drevin et al., 2006; Ruighaver and Maynard, 2006) agree that developing an appropriate IS culture is an effective way to manage user behavior to achieve a more effective IS program. Properly developed communication

channels increase the effectiveness of IS matters on employee behavior (Bess, 2012: 162). What has not been made clear is how to develop and manage an appropriate IS culture. IS culture is defined as the "collective norms, values and beliefs which control the behavior of the individuals within the organization with respect to information systems security" (Van Niekerk and Von Solms, 2010: 478, cited by Bess, 2012). IS culture is considered to be a subculture or a subset of the overall organizational culture (Schlienger and Teufel, 2003), and develops due to behavior of employees, in the same way that an organizational culture develops due to the behavior of employees in the organization (Hellriegel et al., 2001).

Why is Information security culture such an important component to IS? IS programs are ultimately dependent upon the organizational members to implement and maintain the technical and administrative controls in such programs. Because of this dependency, it is the human element that presents the greatest risk to an organization's security program (cited by Bess, 2012: 3). Since it is ultimately the human behavior or people's actions which will operate the IS program then it becomes important to understand how the security-related behaviors of the organizational members can be better understood and governed. Organizational culture has been found to be a significant factor in guiding and governing human behavior within an organization. Early research by Vroom and von Solms (2004) indicated that embedding security practices within the organizational culture could have a positive influence on IS (Vroom and von Solms, 2004). Because of this significant role, organizational culture will influence the operational effectiveness of the IS program (Da Veiga et al., 2007).

3. Research

3.1. Methodology

Qualitative methods have been used in the research because of the purpose of determining the opinions and observations about the control mechanisms of the enterprises or institutions regarding the protection of information security and the continuity of information security by the employees of enterprise. The fact that qualitative methods address a particular context and situation indicates that it is appropriate for the study of interest. According to Gürbüz and Şahin (2014), in qualitative researches, the researcher aims to explore the facts and thoughts in depth by participating in a specific environment as a participant observer in order to find answers to questions such as why, how and who. The reason of preference qualitative research in this study, and its part that differentiates from quantitative studies is the process stage rather than the result. In this research, not only information security applications, but also the observations and experiences about the importance of these applications that affect to the employees and the measures should be taken in order to ensure continuity were also examined. Qualitative studies are frequently preferred methods in description (depiction) situations in social sciences. The model of the research in this context is a descriptive survey model. Such studies are usually carried out in the natural environment, since the situation that exists in descriptive studies is desired to be determined. Techniques used in descriptive studies also change the limitations of the study. These are names such as survey, interview, observation, negotiation (Karasar, 2006).

3.2. Interviews

The sampling method of the research is a sampling of typical situation from the purposeful sampling types. Convenience sampling method is preferred as the research sample among purposive sampling techniques. According to this technique, the researcher collects data by interviewing the appropriate prospective subjects, which are easiest to reach, in order to provide the sample of the time required for the study (Gurbuz and Şahin). The sample of the research is composed of 11 administrators who are active in the chosen task in the environment of interest.In this study, it was preferred to collect data through interview method because of the possibility of getting the in-depth opinions of mid-level and senior managers about information security. The opinions of the staff working as mid-level and top level managers in the institutions are examined within the framework of the themes organized according to the predetermined open ended questions.

- **Perceived Knowledge Level.** Do you and your employees have enough information and awareness about Information Security rules and measures which are applied by your organization
- **The Importance of Taken Precautions**. What is the importance of the these rules and measurements for you, your department and your organization?
- **Behavior and Attitude.** As a department manager, what do you think about the Information Security rules, measures and your employees' attitudes and behaviors according to these?
- **Follow-up and Control of Applicability.** How do you conduct the control and follow up of the implementation of Information Security rules and measures by all employees?
- **Productivity and Efficiency.** What practices can be implemented to increase the level of compliance to the rules and measures and also encourage employees to do so?

The most important way to improve reliability in qualitative research is member control. In this context, researcher' notes are given to the participant and controlled by the participant. In this way, the credibility of the answers is ensured. Internal validity in qualitative studies depends on the fact that the categories and interpretations determined by the research overlap with the actual truths and reflect the reality (Büyüköztürk et al., 2017).

In qualitative studies, the main data collection techniques are negotiations, interviews, documents and semi-structured forms. In interviews the aim is to collect data about the research question. In order for an interview to be assessed qualitatively, it must reflect certain characteristics. A qualitative interview is a discussion on the topic of research, and it is a type of research that the opinions of the experimental subjects about their real life thoughts are pointed out (Gürbüz and Şahin, 2014). In this context, face-to-face interviews were conducted with managers. Interviews were conducted in the workplace environment. Average

time length of interviews were 15-20 minutes. The data came from interviews was further supported by some other office employees.

Yıldırım and Şimşek (2011) stated that the purpose of the qualitative research is having in-depth description and the point of view of negotiator. In the data analysis, it is pointed out that the findings obtained by summing the data according to the specific theme of the descriptive application are presented as of interpreted. From this point of view, descriptive analysis technique, which is often used in qualitative research methods, has been preferred to deeply understand, interpret and regularly reveal the common and disjointed views of managers on information security.

4. Results

4.1. Perceived Knowledge Level

The first sub-question of the research is expressed as "What is the level of knowledge and managers of the information security precautions?" In the context of the sub-question, it is aimed to reveal the level of awareness and knowledge about the information security of managers and employees.

The answers to the question of "information security measures" have not gained a net weight in one direction. If employees have knowledge or haven't knowloedge of this issue is equal to almost half the rate. Some of the answers indicate that employees do not have any specific knowledge of the subject. According to some answers, managers who are asked questions do not seem to have much knowledge about the subject. Some of the answers received are not informed in detail about the information security. Some of the responses received for businesses reported to have adequate knowledge of employees indicates that they are still trying to raise more awareness on employees. While some argue that KVKK practices are sufficient for some of the employees to create awareness on the employees, others have stated that it is sufficient for the information meetings held at more specific periods, or for the attention-grabbing applications. In response to the fact that employees have absolutely sufficient information, it is emphasized that there are audit forms in the related company and that audits are carried out periodically with these forms, and according to another answer, it is stated that explained or written reports to the employees are sufficient to be aware of this issue. According to the size of the institutions in which the study is conducted and the lack of information of the managers who do not have information in their fields of activity is mainly due to the fact that the subject of information security remains in the second plan in their companies. According to the general impression, people who claim that they do not have enough information about information security are more likely to give these answers because their employees haven't enough information on this subject. According to the answers, it is understood that there is no comprehensive training on information security in most enterprises, and the issue remains at the white collar level.

4.1.1. The Importance of Taken Precautions

The first sub-question of the research is expressed as "What is the level of importance that managers give to the precautions applied to information

security?" In the context of the sub-problem, it is aimed to reveal the level of importance that managers and employees give to the measures applied for information security.

All the answers to the question about the importance of the measures taken in Information Security for the Person, Department or institution to which the problem is addressed are of high importance for the information security measures and all concerned people are very aware of the importance of the issue. According to some responses, the first purpose for implementing these measures is to protect the company's information, while others are more afraid of violating personal rights and freedoms or stealing private life information. According to some answers, it is stated that employees should know only what they need to know. It is foreseen that people will be able to have knowledge about matters not included in the job description and to limit the responsibilities and to reach the hands of individuals or institutions that do not have any interest in this kind of information will be reduced to a minimum level. According to some responses, these measures were reported to be of importance only, but no detailed views were given. According to some responses, legal process and legal importance of the subject has been discussed. People who indicate that the subject has importance over its legal dimension and consciousness through legal processes have the impression that the company will be in a difficult situation if new projects and knowhows are transferred to third parties that are vital to the institution in which it is working at the same time. According to some, some sanctions are needed to share information in electronic media in enterprises and the information in digital media must be transferred in a limited manner and only within the authority of the persons. In this way, it is thought that data that may be leaked to third parties can be reduced to a minimum. Although it is seen that some people do not have enough information about information security, it is known by almost everyone how important the issue is for the institutions.

4.1.2. Behavior and Attitude

The first sub-question of the research is expressed as "What is the opinion of the managers about the attitudes of the employees on the application of the rules of information security?" In the context of the sub-problem, it is aimed to present the opinions of the managers on the attitudes of the employees in applying the information security rules.

According to the question of how much information security rules are known or how employees are in attitudes related to the subject, about half of the answers are in the direction that employees show all the sensitivity and dedication to the subject. It emphasizes the importance of sustainability, in other words, to become a culture of sensitivity to the subject. In other words, he emphasized that the issue is not only a matter for today, but also a matter that needs to be addressed with constant sensitivity. According to some responses, it is stated that employees have sufficient awareness about the issue, but it is not possible to take precautions because it is a subject suitable for individual fault. They also stated that although they are aware of the sensitivity in some of the responses, the necessary care was not taken and the employees were insensitive about it. The managers who gave

this response also informed all employees that this was the result although the necessary information was made many times. According to some answers, it is possible to deduce the approach that the subject is known to be superficial but does not understand how important and sensitive it is in detail. For example, it is understood that some employees put their PC passwords on their desks or monitors in post-it form, while others also take notes in notebook or calendar. According to these results, although the majority has awareness, it is understood that there are still deficiencies in practice, that the subject which is thought to be understood is not fully adopted and that it has not yet become a culture within the institution.

4.1.3. Follow-up and Control of Applicability

The first sub-question of the research is expressed as "What are the ways in which managers monitor employees in the context of monitoring and controlling the implementation of information security rules?" In the context of the sub-problem, it is aimed to reveal the ways which administrators monitor, the implementation of information security rules by employees.

A small percentage of respondents to the question of how to follow up and control employees in accordance with the rules set by the enterprises regarding information security prefer deterrence policy directly on the person who violates the security through legal means. A small percentage of the control is provided by periodic inspections and electronic follow-ups. Some people have stated that it is a system developed by the information processing departments of their institutions and that it is prevented from leaking information with this system. In addition to this, a serious rate of follow-up has been provided to employees with information and warnings. The scope of this information is sometimes referred to as the reminder of the rules, and sometimes it is referred to as the legal meaning of the violations. According to the responses received, some businesses notify their employees in writing and form even more binding terms in terms of responsibility. According to a small part of the answers, restrictions have been imposed on the use and sharing of information in digital media in some businesses. In some enterprises, attention was given to the subject, but no details were given. Some of the answers only reported that the process was difficult, while others certainly did not provide follow-up and control. According to the responses, a large part of the institutions concluded that continuous training was given about the subject and that the employee was trying to raise awareness. Some institutions are satisfied with the warnings that documents should not be left in the visible place. Even a small number of organizations have set up a KPI on information security with weekly reporting and follow-up. According to the few answers, the company produced system solutions and continued to remind this information on the corporate company Portal and tried to take steps on the continuity of awareness. Looking at the general table, institutions tried to produce some solutions for information security, albeit in different ways. However, a systematic precaution has not been provided in any company.

4.1.4. Productivity and Efficiency

The first sub-question of the research is expressed as "What are the recommendations of managers to increase the level of application of information security rules?" In the context of the sub-problem, it is aimed to reveal what the recommendations of the administrators are for increasing the level of compliance with information security rules in institutions.

The question of what actions can be taken in relation to increasing the level of compliance with the rules on information security and providing the employees' incentives on the subject was emphasized by the majority of the trainings. With the trainings, briefings, information and meetings to be provided, the importance of the need to explain the importance of the issue is mentioned. A small percentage of the results of the events in this regard are reported to the employees and awareness raising will contribute to the direction. Examples of what happened and material and spiritual gains or losses resulting in positive or negative results can be explained to employees and awareness can be made. These will also be important in terms of ensuring continuity in certain periods. Some of the respondents also believe that personnel should be informed about the legal dimension of the process, among other things. In case of violations, it has been reported how a process will be followed legally and the employees will be informed about the size of the criminal proceedings and an awareness-raising effort can be made. In only one of the answers, some technical practices aimed at encouraging employees are motivated to prevent information sharing. It is stated that more awareness will arise in personnel with the frequency of password change, firewall etc. applications. In general, almost all managers have common opinion that education and derivatives will be essential for employees. In addition, the answer given as a majority can also be interpreted as raising the awareness of the employees through case studies

Conclusion and Recommendations

According to the participants, there was no impression that they had sufficient knowledge of information security in the institutions they worked with. Although some participants report that the employees have sufficient knowledge, it is understood that there is not sufficient level in practice.

Although the employees are aware of the importance of this issue, they have yet to have sufficient awareness in practice. Some participants reported that they understood the importance of the issue by means of legal sanctions. In general, the concept of information security is a very important issue is known by all employees.

The participants gave almost equal answers to the practices of the employees about information security. According to some, the rules were not followed too much, although the importance of the subject was known to behave a little more comfortable in this regard has been reported. According to some, it is reported that the required sensitivity is shown by all employees. In particular, employees in institutions where respondents respond negatively to the issue share their passwords with everyone or leave them in open spaces.

Most of the employees in terms of monitoring and controlling information security practices believe that they provide the necessary control with certain limitations in the digital environment. Some participants have been able to follow this with messages that will generate continuous information and awareness. A small group of participants reported weekly reports and situation control.

The majority of the participants emphasized the importance of education on what incentives can be made and how they can be made to raise awareness of the need for information security employees to show the necessary sensitivity. Information and meetings to be made with frequent periods other than education are often among the answers given in terms of continuity of practice.

According to the general impression, employees in institutions should be informed in more detail about the issue and the importance of the issue should be explained to the employees in case of case studies. Urgent actions should be considered in detail on the extent to which applications can be launched. Employees should be more aware of the legal sanctions of violations and ensure continuity with repeated trainings with frequent intervals. The control and monitoring of the application will be possible with the development of the digital monitoring system and the inspections to be carried out at certain periods.

Although the importance of the education/trainings were emphasized, knowing is not enough by itself. Trainings should be supported with precautions which lead to change of behaviours of employees on showing compliant behaviours. Technology should be used more and applications should be simple and easy.

References

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. International journal of Internet and enterprise management. 6(4): 279-314.

Baars, H., Hintzbergen, J., Hintzbergen, K., & Smulders, A. (2010). Foundations of Information Security Based on ISO27001 and ISO27002, Second edition, Van Haren Publishing, the Netherlands.

Bess, D. A. (2012). Understanding Information Security Culture in an Organization: An Interpretive Case Study. (3526079 Ph.D.), Nova Southeastern University, Ann Arbor. https://search.proquest.com/docview/1039269451

Björck, F. (2004). Institutional Theory: A New Perspective for Research into IS/IT Security in Organisations. Paper presented at the 37th Hawaii International Conference on System Sciences (HICSS). Hawaii. 5-8 January 2004. Cited by Coles-Kemp, (2009).

Büyüköztürk, Ş., Çakmak, E. K., Akgün, Ö. E., Karadeniz, Ş., & Demirel, F. (2017). Bilimsel araştırma yöntemleri. Pegem Atıf İndeksi, 1-360.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems. 106(3): 345-361.

Coles-Kemp, L. (2009). Information security management: An entangled research challenge. Information Security Technical Report. 14(4): 181-185.

Da Veiga, A., Martins, N., & Eloff, J. H. (2007). Information security culturevalidation of an assessment instrument. Southern African Business Review. 11(1): 147-166.

Davies, H. T., Nutley, S. M., & Mannion, R. (2000). Organisational culture and quality of health care. Quality in Health Care. 9(2): 111-119.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. Communications of the ACM. 43(7): 125-128.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management, Journal of Information Security, Volume 4, No 2, 92-100.

Drevin, L., Kruger, H., & Steyn, T. (2006). Value-Focused Assessment of Information Communication and Technology Security Awareness in an Academic Environment. Computers & Security. 26: 36-43.

Duffy, N. M., & Assad, M. G. (1980). Information management: an executive approach. Oxford University Press, USA.

Dunkerley, K. D. (2011). Developing an Information Systems Security Success Model for Organizational Context. (3456547 Ph.D.), Nova Southeastern University, Ann Arbor.

Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. California Management Review. 45(1): 67-87.

Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. Computer Fraud & Security. 2005(11): 10-16.

Farradane, J. (1979). The Nature of Information, Journal of Information Science, Volume 1, No 1, 13-17.

Fulford, H., & Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. Information Management & Computer Security. 11(3): 106-114.

Gerber, M., & von Solms, R. (2008). Information security requirements ± Interpreting the legal aspects. Computers & Security. 27(5±6): 124-135.

Gürbüz, S., & Şahin, F. (2014). Sosyal bilimlerde araştırma yöntemleri. Ankara: Seçkin Yayıncılık.

Hellriegel, D., Slocum Jr, J., & Woodman, R. (2001). Organizational Behavior. Mason, OH: Thomson Learning, South-Western College Publishing.

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. Information Management & Computer Security. 11(5): 243-248.

Iivari, J., & Hirschheim, R. (1996). Analyzing information systems development: A comparison and analysis of eight IS development approaches. Information Systems. 21(7): 551-575.

ISO/IEC 27001:2013 Information Technology – Security techniques – Information Security Management Systems – Requirements, 2013, Second Edition, published in Switzerland.

Ives, B., & Olson, M. H. (1984). User involvement and MIS success: a review of research. Management science. 30(5): 586-603.

Kankanhalli, A., Teo, H.-H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management. 23(2): 139-154.

Karasar, N. (2006). Bilimscl Arastirma Yöntemi. 16. Baski, Ankara: Nobel Yayincilik.

Lacey, D. (2010). Understanding and transforming organizational security culture. Information Management & Computer Security. 18(1): 4-13.

Lampson, B. W. (2004). Computer security in the real world. Computer. 37(6): 3746.

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: a parsimonious framework. Information Management & Computer Security. 16(3): 251-270.

Mader, A., & Srinivasan, S. (2005). Curriculum development related to information security policies and procedures. Paper presented at the 2nd annual conference on Information security curriculum development. Kennesaw, GA. 23-24 September 2005.

Meta Security Group. (2000). Information Security Policy Framework. https://horseproject.wiki/images/1/18/Information-Security-Policy-Framework-Research-Report.pdf

National Institute of Standards and Technology. (2004). Standards for Security Categorization of Federal Information and Information Systems, Federal Information Procesing Standards Publication, FIPS Publication 199, Gaithersburg.

Perks, C., & Beveridge, T. (2003). Guide to enterprise IT architecture. New York, NY: Springer.

Pettigrew, A. M. (1979). On studying organizational cultures. Administrative science quarterly. 24(4): 570-581.

PricewaterhouseCoopers. (2013). 2013 US State of Cyber Crime Survey. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58738

Reason, J. T. (1997). Managing the risks of organizational accidents (Vol. 6): Ashgate Aldershot.

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: a policy framework for information security. Communications of the ACM. 46(7): 101-106.

Rotvold, G. (2008). How to create a security culture in your organization. Information Management Journal. 42(6): 32-38.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. Computers & Security. 26(1): 56-62.

Schein, E. H. (1985). Organisational culture and leadership: A dynamic view. San Francisco, CA: Jossey-Bass.

Schein, E. H. (1988). Organizational culture. http://dspace.mit.edu/handle/1721.1/2224

Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. 14th International Workshop on Database and Expert Systems Applications, 2003 (pp. 405-409): IEEE.

Schweitzer, J. A. (1987). How security fits in a management view: Security is an essential for quality information. Computers & Security. 6(2): 129-132.

Scott, T., Mannion, R., Davies, H., & Marshall, M. (2003). The quantitative measurement of organizational culture in health care: a review of the available instruments. Health services research. 38(3): 923-945.

Sheikhpour, R., & Modiri, N. (2012a). "An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls", International Journal of Security and Its Applications, Vol. 6, No. 2, 13-27.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. Communications of the ACM. 49(8): 97-100.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security. 8(1): 31-41.

Sittig, D. F., & Singh, H. (2010). A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. Quality and Safety in Health Care. 19(Suppl 3): 168-174.

Smit, J., & Dellemijn, M. (2011). The Relationship Between Information Systems Management and Organizational Culture. Communications of the IIMA. 11(3): 21-33.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. MIS quarterly. 22(4): 441-469.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five, International Journal of Electrical and Computer Sciences IJECS-IJENS, Vol. 11, No. 5, 21-27.

Tang, J. (2008). The Implementation of Deming's System Model to improve Security Management: A Case Study. International Journal of Management. 25(1): 54.

The Stationary Office (2017a). ITIL Service Strategy, the 2011 Edition, the United Kingdom.

The UK Chapter of the itSMF Ltd (2017). An Introductory Overview of ITIL V3 2011, Published by the Stationery Office.

Theodorakis, Y. (1994). Planned behavior, attitude strength, role identity, and the prediction of exercise behavior. Sport Psychologist. 8(2): 149.

Torres, J. M., Sarriegi, J. M., Santos, J., & Serrano, N. (2006). Managing information systems security: critical success factors and indicators to measure effectiveness. Information Security (pp. 530-545): Springer.

Trcek, D. (2003). An Integral Framework for Information Systems Security Management. Computer & Security, 22, 337-360.

Tudor, K. J. (2002). Information security architecture: an integrated approach to security in the organization. Boca Raton, FL: CRC Press.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security. 23(3): 191-198.

Waly, N., Tassabehji, R., & Kamala, M. (2012). Measures for improving information security management in organisations: the impact of training and awareness programmes. Paper presented at the UK Academy for Information Systems Conference Proceedings 2012.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security. 17(1): 4-19.

Williams, P. (2008). A practical application of CMM to medical security capability. Information Management & Computer Security. 16(1): 58-73.

Winkel, O. (2007). Electronic government and network security: a viewpoint. Transforming Government: People, Process and Policy. 1(3): 220-229.

Yıldırım, A., & Şimşek, H. (2011). Sosyal bilimlerde nitel araştırma yöntemleri. Ankara: Seçkin Yayıncılık.

http://www.merriam-webster.com/dictionary/security

http://www.utica.edu/faculty_staff/qma/needforsecurity.pdf

https://hackjacks.blogspot.com.tr/2014/10/cia-triad-for-base-of-information.html

https://hazelturan.wordpress.com/2016/03/03/the-interactions-in-between-itil-cobit-and-iso27001/

SRA Strategic Research Academy ©