Evaluation of IT Security Perception

Full Paper

Nur Sena Tanrıverdi
Management Information Systems Dept.,
Bogazici University
nur.tanriverdi@boun.edu.tr

Bilgin Metin
Management Information Systems Dept.,
Bogazici University
Bilgin.metin@boun.edu.tr

Abstract

Information Technology security is an important issue that companies ensure with using technical solutions most of the time. However, protection cannot be completely beneficial unless human factor is considered carefully. Technical solutions are successful together with non-technical solutions, such as security education/training programs which target to users. These activities are planned to improve knowledge of users and improve their secure behavior through increasing information security awareness about IT security. In this study IT security perception, awareness and behavior are evaluated together so as to understand how employees perceive IT security according to their professions from the point of IT security literacy. Furthermore, results are compared with global information security surveys to expand the understanding.

Keywords

Information security perception, information security awareness, information security behavior.

Introduction

Information technology (IT) systems are used in variety of ways including transmission, storage and data processing in all organizations regardless their size. That's why companies take a big care of the security of their vital assets; IT systems. Security of the IT systems is provided by using technical solutions like authentication, cryptography, advanced firewalls etc. against to attacks. However, technical solutions cannot achieve to protect systems completely when human factor is ignored (Johnson, 2006). Non-technical solutions, such as information security education and training programs can be helpful to provide comprehensive protection. These methods increase the knowledge of users and improve their daily interaction with IT systems through increasing information security awareness.

The protection of IT systems from different security attacks is a constant challenge that many organizations face because of technological developments (Karyda, Kiountouzis and Kokolakis, 2005). Advances in technology increases variety of threats and affect the way that users interact with technology (Kruger and Kearney, 2006). This situation shows critical role of employees in the IT security.

Controlling the human element of security plays an important role in a company. To understand the human element, it is vital to understand perception, awareness, attitude, behavior, knowledge of human in terms of information security. Awareness can be considered as an impact on perception defined as "the ability to see, hear and become aware of something through senses" (Oxford Dictionaries). Moreover, information security awareness means knowing both existence of threats and protection methods (Hansch and Benenson, 2010). From another point of view, main components of information security awareness are general information security awareness and information security policy awareness (Bulgurcu, Cavusoglu and Benbasat, 2010). Definition of general information security is that "an employee's overall knowledge and understanding of potential issues related to information security and their ramifications". Awareness is also described in three dimensions as knowledge, attitude and behavior (Kruger and Kearney, 2006); "What does a person know" corresponds to knowledge, "how do they feel about the topic" is attitude and "what do they do" is behavior.

In this study IT security perception, awareness and behavior are evaluated together with a survey. IT security perception is measured with what employees know insider and outsider related security problems in their companies. Also, their knowledge about useful protection methods is evaluated under IT security perception. Analyses of attitude towards sharing login information and unauthorized access are considered under IT security awareness. Additionally, IT security behavior of employees are meas-

ured with backing up of data, using antivirus, logging off computer system after working, and opening unknown link and e-mail attachments. Our approach testing these fundamental points is known as "IT security literacy" (Wilson, de Zafra, Pitcher, Tressler and Ippolito, 1998).

In this study, different from the literature, we focused on the impact of employee professions, that is classified as IT and non-IT, on the security perception, awareness, behavior. Also, survey results are presented and classified by professions.

Following hypotheses are built based on our approach in this study:

H1: There is a relationship between profession of employee and employee's knowledge about insider based IT security problems

H2: There is a relationship between profession of employee and employee's knowledge about outsider based IT security problems.

H3: There is a relationship between profession of employee and employee's awareness about login information security

H4: There is a relationship between profession of employee and their opinion about unauthorized access

H5: There is a relationship between profession of employee and their back-up behavior

H6: There is a relationship between profession of employee and their antivirus software usage

H7: There is a relationship between profession of employee and their logging off computer behavior

H8: There is a relationship between profession of employee and their behavior on opening unknown e-mail attachments and links

This paper is organized as follows. In the Literature Review section, reviewed literature related to information security perception, awareness and behavior are summarized. Data Collection and Analyses section explains briefly the methodology of this study. Then, Results section outputs of hypothesis tests are given. Test results are analyzed with different perspectives in Discussion section, also comparison with global security survey result are provided in the section. Finally, Conclusion summarizes outcomes of this study. Moreover, questionnaire of this study and detailed Cross Tabulation test results are provided in Appendix B.

Literature Review

In this study, we concentrate on employee professions with "IT security literacy" (Wilson, de Zafra, Pitcher, Tressler and Ippolito, 1998). Also other approaches are possible. Some of the information security awareness studies focused on behavioral information security theories. Also some studies investigate effective factors of information security policy compliance. Furthermore, information security awareness education is analyzed many times in the literature.

Existent literature shows that relationship between information security behavior and information security awareness is investigated many times. Models based on behavioral information security theories are examined to explain the effect of information security awareness to behavior of people. A theory-based literature review study has been conducted by Lebek et al. This literature review study collects theory-based information security awareness and behavior studies (Lebek et al., 2014). It summarizes which theories are investigated in information security literature, how many times they are studied. According to this study the most frequent theories are respectively Theory of Reasoned Action (TRA)/Theory of Planned Behavior (TPB), General Deterrence theory (GDT), Protection Motivation Theory (PMT), Technology Acceptance Model (TAM), although they identified 54 different studies in the literature. These theories are adopted to information security area from different disciplines, such as psychology, sociology and criminology (Bulgurcu, Cavusoglu and Benbasat, 2010), (Hu and Dinev, 2007), (Ifinedo, 2012), (Pahnila et al., 2007), (Hu et al., 2012).

Information security behavior is usually considered as behavior that comply with information security policy of a company in the literature. Effective factors on information security compliance (information security policy compliance) are also searched in information security literature. In addition to this, those factors are evaluated based on the theories (Bulgurcu, Cavusoglu and Benbasat, 2010), (Pahnila et al., 2007), (Hu et al., 2012).

Some combinations of the theories are synthesized to fulfill the research gap in the literature (Bulgurcu, Cavusoglu and Benbasat, 2010), (Herath and Rao, 2009), (Ifinedo, 2012), (Hu and Dinev, 2007).

In the literature information security education is analyzed many times. As it is mentioned in Global Information Security Survey which has been conducted by Ernst and Young in 2004, lack of awareness of users is seen as a serious obstacle for effective information security (Johnson, E.C., 2006). That's why companies need to give security awareness education and training programs for all employees regardless their departments. Researchers analyzes what security education aims to teach (May, 2008). Some studies concluded as after giving proper security awareness education and training, improvement in security awareness and behavior of users is expected through enhance their understanding about what security risks and threats are, and how they can protect information systems of company (Albrechtsen and Hovden, 2010), (Hansch and Benenson, 2010), (Eminagaoglu, Ucar and Eren, 2009).

Data Collection and Analyses

The research participants are employees of companies in Turkey. Survey was conducted in the middle of 2013. Companies were randomly selected for the survey. Then the companies were requested to participate. Web based survey was sent them by email. A total of 243 employees participated to the survey. Any participant was not excluded because of incomplete answers. Questions were not mandatory to answer. Therefore, total number of responses which is given for each question is mentioned in tables of this paper. Missing cases are not included in percentages.

Survey questions were developed in nominal scale except the question asking company size. Company size question was in ordinal scale. Questionnaire includes self-developed questions and questions adapted from other researches.

Cross Tabulation analyses were conducted so as to test hypotheses. Cross tabulation analyses were conducted with at most 178 participants because of classification according to professions of employees. Detailed test results are given in Appendix B. Moreover, bar charts given for each test results to illustrate rates of answers, such as 'yes', 'no' and 'not sure', and also answers of respondents classified by professions given in percentages.

Participants of our survey are employees working in at least 82 different companies of Turkey. Majority of the industry of participants' companies are respectively telecommunication, finance/banking, education and insurance sector. 22.2% of all participants are working in telecommunications sector while 21% of all participants are from finance, banking and insurance sector (Table 1).

Industry	Frequency	Percentage	Industry	Frequency	Percentage
Telecommunications	54	22.2	Logistics, transportation	5	2.1
Finance, banking	33	13.6	Health & medicine	5	2.1
Education	18	7.4	Travel & leisure	5	2.1
Insurance	18	7.4	Manufacturing	3	1.2
R&D	10	4.1	Law, management consulting	2	0.8
Automotive	9	3.7	Food & beverage	2	0.8
Entertainment, media	8	3.3	Real estate, construction	1	0.4
Retail sales	6	2.5	Other	59	24.3
Energy	5	2.1	Total	243	100

Table 1. Industry of Companies

Majority of the participants, 39.3% of them, are coming from company that has more than 500 employees (Table 2). However, attendance of employees from all determined size of companies is satisfying.

Size	Frequency	Percentage	Size	Frequency	Percentage
0-10	19	7.9	251-500	18	7.5
11-50	53	22.2	More than 500	94	39.3
51-250	55	23.0	Total	239	100

Table 2. Size of Companies

Professions of the participants were asked. According to the survey results 69.1% of participants (123 participants) are working at IT related professions as system administrator, software developer, project manager, IT consultant, IT personnel, web designer, database administrator, system analyst and business analyst. On the other hand rest of them (55 participants that constitutes 30.9% of participants) have a job in department not related to IT; finance & accounting, sales & marketing, human resources and after sales departments. 26.7% of all participants (65 participants) have mentioned their professions as 'other'. So, they were excluded from the classification, so their answers were not evaluated questions which professions have been analyzed.

Results

Hypotheses test results and frequency analyses of questionnaire, given in Appendix A, are provided in this section. According to test results there is not significant relationship between variables which constitute hypotheses *H1, H3, H4, H5, H6, H7* and *H8*. On the other hand Hypothesis *H2* is validated.

IT Security Perception

Employees' perceptions are evaluated with what they know about suffered IT security problems in companies. Also their knowledge about useful IT security protection methods for their companies is also considered within IT security perception.

IT Security Problems

IT Security problems can be caused by both insiders and outsiders. Whether companies have suffered problems from insider or outsider is asked to participants to show what they know about IT security problems of their companies and does perception of them change based on their professions are investigated.

Insider Based IT Security Problems: Whether company had any staff related security problems was asked to participants. As it is shown in Figure 1, 51.98% of all participants (177 people) mentioned that their company didn't have any staff related security incident. Only 19.77% of them said that they had. According to the Cross Tabulation results there is not a significant relationship between given answer of staff related security question and profession of employee, because significance level is 0.159, as it is seen in Appendix B.

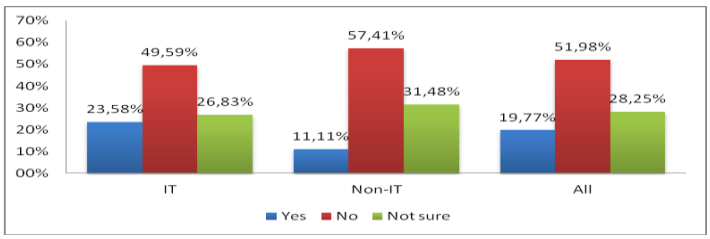

Figure 1. "Have you suffered a staff related security incident?"

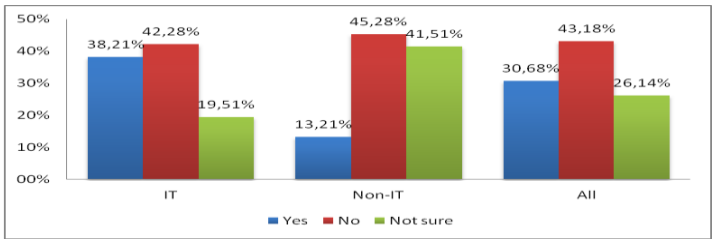

Figure 2. "Were your company's systems attacked by an outsider in the last year"?

Outsider Based IT Security Problems: Participants have been asked whether their companies were attacked by outsiders. 43.18% of 176 respondents said 'No' while 30.68% of them said 'Yes'. As it can be understood from Figure 2, there is not a slight difference between the given answers by IT employees and non-IT employees. Answers of non-IT employees are respectively 'no', 'not sure' and 'yes' whereas IT employees' are 'no', 'yes' and 'not sure'. Cross Tabulation

results also show that there is a significant relationship between given answers and professions of employees. Chi-square level is 0.001 which is acceptable level (Appendix B).

Useful Protection Methods According to Employees

Participants were asked most useful protection methods for organizations to see how they perceive security measures. As it is seen in Table 3, 622 answers were given totally. There are different methods mentioned in options. The most selected option is network security with 174 choices. The second most preferred method is public security awareness with 119 choices. On the other hand, the least preferred protection methods are cloud security and mobile security with less than 30 times.

Item	Frequency	Item	Frequency
Network security	174	Risk management	42
Public security awareness	119	Cloud security	27
Disaster recovery	92	Mobile security	16
System security	90	Total	622
Penetration testing	62		

Table 3. "What assistance would be most useful to you to help protect your company? "

IT Security Awareness

In this part IT security awareness of employees is aimed to be evaluated. Whether IT employees are more aware than non-IT employees is also examined according to questions given in this part.

Awareness questions which ask opinions of participants directly about such security issues as revealing personal login information, unauthorized access to company network were asked in the questionnaire. Research clearly shows that sample population is quite aware of the importance of questioned security issues, although relationship between awareness of employees and their professions are not proven.

Sharing Login Information: Whether participants perceive sharing their own login information with other people as a potential problem was questioned. Awareness about sharing private user information like password and user name is not related to employees' profession because Chi-Square test results show that significance level (0.910) is not satisfying (Appendix B). It means there is no significant relationship between keeping login information secret and profession of employees. Results of the question is given in Figure 3.

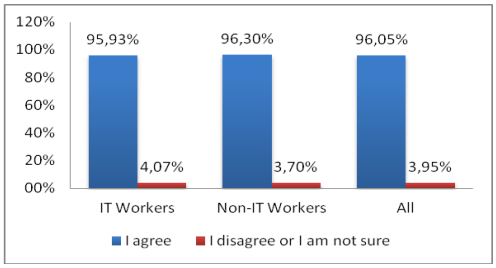

Figure 3. "I believe that it is not safe to reveal my login information to anyone, for any reason."

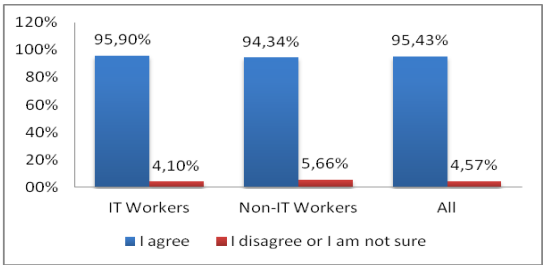

Figure 4. "It should be banned to access the network of company for an unauthorized user."

Unauthorized Access: What employees think about authorized access was questioned. Participants are also aware about authorized access regardless their professions. Totally 175 participants are used for the analysis here. As it is seen in Figure 4, 95.43% of all respondents mentioned that access of unauthorized user to company's network should be banned. Significance level of Chi-Square test is 0.649 (Appendix B), so it shows that there is not an important relationship between awareness about unauthorized access to company network and profession of an employee.

IT Security Behavior

Following analyses belongs to questions which aim to measure employees' IT security related behaviors. These behaviors are especially on back up of data, using antivirus, locking computer system, opening unknown link and e-mail attachments. It is analyzed that participants' behaviors are appropriate in terms of IT security protection regardless their professions or not.

Back-up: Losing of personal data or its corruption is serious data security problem, so back-up is vital protection method (Wilson, de Zafra, Pitcher, Tressler and Ippolito, 1998). When it is asked to employees, 80.70% of 171 participants mention that they do back-up their personal data on removable storage media and 19.30% of them don't back-up (Figure 5). According to the Chi-Square Test significance level is 0.565, so back-up behavior is not related to whether employees' job related to IT (Appendix B).

Antivirus Solutions: It has been aimed to learn how employees' antivirus usage at home computer. As it is seen in Figure 6, 88.30% of 171 participants use antivirus software at home computer. But there is not a significant relationship between antivirus usage and profession of employees. Because significance is, 0.576, not satisfying according to the Chi-Square test (Appendix B). However, this result can be accepted satisfying within employees' secure behaviors about antivirus usage, if professions are regarded.

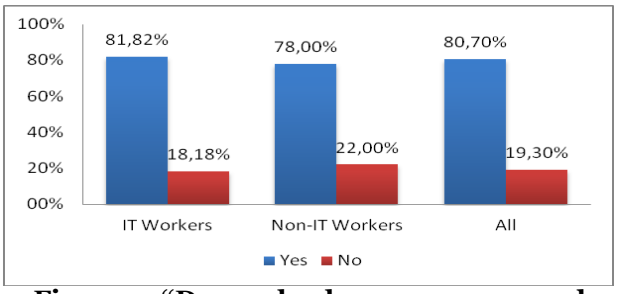

Figure 5. "Do you back-up your personal data on removable storage media (such as disks. CDs)"

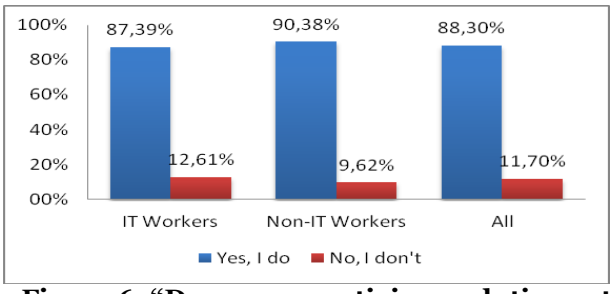

Figure 6. "Do you use antivirus solutions at your personal computer at home?"

Log off: To ensure nobody have access to your system or use your login account, logging off or locking is necessary behavior although there are automatized settings like locking computer system after 30 minutes of inactivity. Usual behavior of employees at working environment was asked with the question. 177 responses are tested with Cross-Tabulation. 95.48% of all respondents mentioned that they lock their computer system or turn off it when they leave from their office. Both are desired behaviors. Rest choices; turning off monitor/programs and leaving the system on are grouped together and these options have risk in terms of security. Percentage of each action is given in Figure 7. Results show that the vast majority of participants behave secure in office environment in terms of logging of their PCs. Moreover, there is no relationship between locking behavior and profession of employees, as it is seen in Appendix B significance level of Chi-Square test is 0.66.

Opening Email Attachments and Links: Participants' behavior about opening email attachments or links from unknown sender were questioned. Cross tabulation analysis was conducted with 178 responses. According to the results 53.37% of participants behave appropriately in terms of security, they mention that they 'never' open email attachments or links coming from unknown sender. 39.89% of them mention that they 'rarely' open while 6.74% of them 'usually' open (Figure 8). In addition, significance level is 0.906 (Appendix B), so behavior about opening links and email attachments from unknown sender is not related to employees' profession.

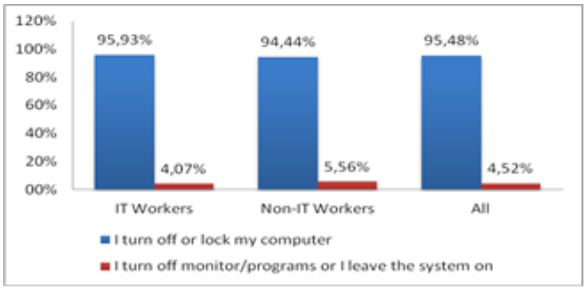

Figure 7. "When you leave your office, what do you usually do with your computer?"

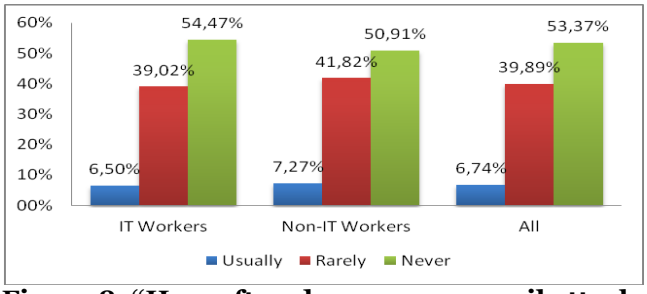

Figure 8. "How often do you open email attachments or links that you receive from unknown sender?"

Discussion

In this section, test results are analyzed with different perspectives and also compared with global security survey result (ISACA, 2016), (Deloitte, 2013), (PwC, 2016). After testing hypotheses, following points are found important and worth to analysed deeply.

Professions' Effects on Known Security Problems

Security problems suffered at companies caused by insiders and outsiders were asked to employees. The most important result is that known insider related security incidents are not dependent on employees' professions, whereas known outsider related security issues depend on professions according to the cross tabulation results.

Basically outsiders target to harm technological assets of companies and technological assets are under IT staff's responsibility, so outsider attacks are known by IT staff only. Because of this situation companies should inform IT staff about outsider related incidents. On the other hand, companies warn all staff regardless their departments about staff related security incidents to interrupt the repetition of the incident. It can be considered as a reason of that knowing insider based problems is independent from professions of employees.

According to participants of ISACA's 2016 Cybersecurity Snapshot Survey (ISACA, 2016) social engineering, insider threats and advanced persistent threat are respectively the most important consideration for their organization in 2016. Intentional or unintentional actions of people are the biggest threat of organizations. Additionally, The Global State of Information Security Survey 2016 of PwC (PwC, 2016) shows that current employees have threatened companies at most. 34% of security incidents in 2015 have been caused by current employees according to results of the survey. These results and our results support each other.

Useful Protection Methods According to Employees

Except measuring IT perception with taking what they know about security problems, which protection methods they find useful is used as a dimension of IT security perception. Network security and public security awareness are respectively perceived as the most useful protection methods. It shows that they perceive how vital the role of users in IT security. The result also supports TMT Global Security Study conducted in 2013 by Deloitte. The study reveals that according to 70% of study participants lack of sufficient awareness with employees has been perceived as average or high threat (Deloitte, 2013).

On the other hand, the least preferred protection methods are cloud security and mobile security. This result may be caused by insufficient usage of these relatively new technologies in companies in Turkey.

IT Security Awareness and Behavior of Employees

When it comes to information security awareness, results are satisfying because employees are quite aware of providing security of systems. Moreover, IT security behavior of employees are safe according to results. The most important result about awareness and behavior is that information security awareness and behavior of employees are independent from professions.

First of all losing of personal data or its corruption is perceived as serious data security problem, so participants do back-up their personal data. Moreover, a great majority of participants use antivirus

software at home computer. It may be caused by that antivirus software is usually default software of computers.

Other issue is sharing login information. To ensure nobody have access to your system or use your login account, vast majority of respondents lock their computer system or turn off it when they leave from their office. Employees can be seen cautious about security inside of their companies.

Last security behavior is opening email attachments or links from unknown sender. Although more than half of the participants claimed that they never open unknown mail, nearly 40% of them said they rarely open. It is desired not to get that much response with 'rarely' because desired behavior is their absolute avoidance of opening links/attachments from unknown senders. However, people can recognize harmful emails that is why they 'rarely' open those emails. In other words, determination of whether sent email is risky and the sender is completely stranger is possible (Power and Forte, 2006). In information security awareness education the methods of how to determine harmful senders, links and emails are given. They may not threat computer systems, even though they rarely open unknown email attachments and links.

Conclusion

In this study we emphasized the importance of the IT security literacy that is the core knowledge set needed to protect electronic information systems from the point of employee profession. IT security literacy is the ultimate goal of the IT department to improve IT security. In our study participants' awareness and behaviors are satisfying. At least their daily usage doesn't create risk. Furthermore, executing fundamental security actions don't depend on whether they are IT related worker. That is why even if hypotheses are not proven except H2, results are satisfactory on behalf of Turkish companies.

Although IT security literacy of employees is enough to conduct basic IT security activities, actual security profile of companies in Turkey cannot be drawn with looking of every employee's response. Because it is seen from the results that what employees know about security is changed according to their professions. Knowing outsider related security problems, which is more technical issue, is related to department of employee, whereas there is no relationship between knowing insider related security incidents and professions of employees.

Which security problems are known by employees can be associated with how frequent employees come across the same problem and whether they are able to prevent its repeat. When company had a phishing attack, company should announce this issue to all employees. Because, all employees are target of phishing attack. They should know suffered problem to avoid the repeat of the same problem in the company. At this point information security perception can be improved by not only IT security education/training programs but also such frequent activities as desk-to-desk alerts, web based sections, newsletters and informative emails etc.

Appendix A: Source of Survey Questions

Survey Item	Source
Have you suffered a staff related security incident?	Adapted from (Vroom and von Solms, 2004)
What assistance would be most useful to you to help protect your organization? Were your company's systems attacked by an outsider in the last year?	Adapted from (Whitman, 2003)
It should be banned to access the network of company for an unauthorized user. I believe that it is not safe to reveal my login information to anyone, for any reason.	Adapted from (Kruger and Kearney, 2006)
How often do you open unexpected files or e-mail attachments or files, that you receive form unknown sender. Do you back-up your data on removable storage media (such as disks, CDs) Do you use antivirus solutions at your personal computer at home? When you leave your office, what do you usually do with your computer?	Adapted from (Wilson and Hash, 2003)

Appendix B: Chi-square test results of cross tabulation analyses

Pearson Chi-Square / Item	Value	df	Asymp. Sig. (2-sided)
"Have you suffered a staff related security incident?"	3,677	2	0,159
"Were your company's systems attacked by an outsider in the last year?"	14,482	2	0,001
"It should be banned to access the network of company for an unauthorized user."	0,207	1	0,649
"I believe that it is not safe to reveal my login information to anyone, for any reason."	0,013	1	0,910
"Do you use antivirus solutions at your personal computer at home?"	0,313	1	0,576
"Do you back-up your personal data on removable storage media (such as disks, CDs)"	0,331	1	0,565
"How often do you open email attachments or links that you receive from unknown sender?"	0,198	2	0,906
"When you leave your office, what do you usually do with your computer?"	0,193	1	0,660

REFERENCES

Albrechtsen, E., and Hovden, J. 2010. "Improving Information Security Awareness and Behaviour through Dialogue, Participation and Collective Reflection. An Intervention Study," *Computers & Security* 29, pp. 432-445.

Bulgurcu, B., Cavusoglu, H., and 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.

_ English_final_020113.pdf (visited on 19/04/2017).

Deloitte, 2013. "Blurring the lines 2013 TMT Global Security Study," URL: http://www2.deloitte.com/content/dam/ Deloitte/ global/Documents/ Technology-MediaTelecommunications/dttl_TMT_GlobalSecurityStudy _ English_final_020113.pdf (visited on 19/04/2017).

Eminagaoglu, M., Ucar, E., and Eren, S. 2009. "The Positive Outcomes of Information Security Awareness Training in Companies – A Case Study," *Information Security Technical Report*, (14:2009), pp. 223-229.

Hansch, N., and Benenson, Z. 2014. "Specifying IT Security Awareness," *25th International Workshop on Database and Expert Systems Applications, IEEE Press,* Munich, pp. 326-330.

Herath, T., and Rao, H. G. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems,* (18:2), pp. 106-125.

Hu, Q., and Dinev, T. 2007. "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," *Journal of the Association for Information Systems*, (8:7), pp. 386–408.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. "Managing employee compliance with information security policies: the role of top management and organizational culture," *Decision Sciences*, (43:4).

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.

ISACA, "January 2016 Cybersecurity Snapshot Global Results," URL: http://www.isaca.org/cyber/ Documents/2016-Global-Cybersecurity-Snapshot-Data-Sheet_mkt _Eng _0116.pdf (visited on 19/04/2017).

Johnson, E.C. 2006. "Security Awareness: Switch to a Better Programme" *Network Security* 15-18.

Karyda, M., Kiountouzis, E., and Kokolakis, S. 2005. "Information Systems Security Policies: a Contextual Perspective," *Computers & Security* (24:3), pp. 246-260.

Kruger, H.A., and Kearney, W.D. 2006. "A Prototype for Assessing Information Security Awareness," *Computers & Security* (25:4), pp. 289-296.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., and Breitner, M. H. 2014. "Information Security Awareness and Behavior: A Theory-Based Literature Review," *Management Research Review* (37:12), pp. 1049-1092.

May, C. 2008. "Approaches to User Education." *Network Security* 15-17.

Oxford Dictionaries, URL: http://www.oxforddictionaries.com/definition/english/perception (visited on 06/08/2015).

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study," *PACIS 2007 Proceedings*, 73.

Power, R., and Forte, D. 2006. "Social Engineering: Attacks Have Evolved, but Countermeasures Have not," *Computer Fraud & Security* (2006:10), pp. 17-20.

PwC, "Key Findings from The Global State of Information Security Survey 2016," URL: https://www.pwc.com.tr/tr/risk-surec-teknoloji-hizmetleri/bilgi-guvenligi-ve-siber-guvenlik-yayinlari/siber-riskleri-firsata-donusturme-zamani.pdf (visited on 19/04/2017).

Vroom, C. and von Solms R. 2004. "Towards Information Security Behavioral Compliance," *Computers and Security* (23:3), pp. 191-198.

Wilson, M., de Zafra, D.E., Pitcher, S.I., Tressler, J.D. and Ippolito, J.B. 1998. "Information Technology Security: Training Requirements: a Role and Performance Based Model," *NIST SP 800-16*.

Wilson, M., and Hash, J. 2003. *Building an Information Technology Security Awareness and Training Program*. NIST SP 800-50.

Wolf, M., Haworth, D., and Pietron, L. 2011. "Measuring an Information Security Awareness Program," *Review of Business Information Systems Third Quarter 2011* (15:3), pp. 9-21.

Whitman, M. 2003. "Enemy at the Gate: Threats to Information Security," *Communications of the ACM* (46:8), pp. 91-95.