

THE EFFECT OF EMPLOYEES' INFORMATION SECURITY FAMILIARITY
ON THEIR SECURITY INCIDENT AWARENESS

NUR SENA TANRIVERDİ

BOĞAZIÇI UNIVERSITY

2018

THE EFFECT OF EMPLOYEES' INFORMATION SECURITY FAMILIARITY
ON THEIR SECURITY INCIDENT AWARENESS

Thesis submitted to the
Institute for Graduate Studies in Social Sciences
In partial fulfillment of the requirements for the degree of

Master of Arts
in
Management Information Systems

by
Nur Sena Tanrıverdi

Boğaziçi University

2018

DECLARATION OF ORIGINALITY

I, Nur Sena Tanrıverdi, certify that

- I am the sole author of this thesis and that I have fully acknowledged and documented in my thesis all sources of ideas and words, including digital resources, which have been produced or published by another person or institution;
- this thesis contains no material that has been submitted or accepted for a degree or diploma in any other educational institution;
- this is a true copy of the thesis approved by my advisor and thesis committee at Boğaziçi University, including final revisions required by them.

Signature.....

Date11.06.2018.....

ABSTRACT

The Effect of Employees' Information Security Familiarity on Their Security Incident Awareness

Finding more sophisticated and effective solutions to protect data and information systems against advanced security threat is essential in both theory and practice. Technologies and laws are evolved to have more useful, robust and smarter protection methods. Also, researchers investigate human element of information security to measure people's behavior and security awareness level. In this study, whether employees are capable to be a part of information security protection in their companies is investigated. Firstly, effect of information security familiarity on security incident awareness is discussed, then how security incident awareness affects security behavior is attempted to analyze. Implications of this study can help to improve employees' behavior without any distinction between professions as well as information security awareness education and training programs. For this purpose, detailed literature review has been conducted and research model has been developed. Primary data source of this study is a survey. In order to develop questions for the survey, security experts' opinion has been consulted besides literature studies. An online survey has been conducted on employees who work in companies located in Turkey. Totally 315 responses have been used to conduct analyses which have been applied to test five hypotheses proposed in this study.

ÖZET

Çalışanların Bilgi Güvenliği Aşinalıklarının Güvenlik Olay Farkındalıkları Üzerine Etkisi

Hem akademik araştırmalarda hem de sektör uygulamalarında bilgi ve bilgi sistemlerini, gelişmiş güvenlik tehditlerine karşı daha efektif ve sofistike yöntemler ile korumanın yollarını bulmak asıl hedeftir. Teknoloji ve yasalar, koruyucu yöntemler için daha akıllı, kullanışlı ve dirençli bir zemine sahip olmak adına geliştirilmektedir. Ayrıca araştırmacılar güvenliğin insan unsurunu, kişilerin davranış ve güvenlik farkındalık düzeylerini ölçmek ve değiştirebilmek için incelemektedirler. Bu eforun arkasındaki sebep, günümüzde ve yakın gelecekte daha çok dijitalleşmiş ortamlara sahip olmamızdır. Bu çalışmada, çalışanların daha fazla dijitalleşmiş bir ortamda bilgi güvenliğinin bir parçası olmaya ne kadar hazır olduklarının görülmesi hedeflenmiştir. Bilgi güvenliği aşinalığının, güvenlik olay farkındalığı üzerindeki etkileri araştırılmış, ardından güvenlik olay farkındalığının güvenlik davranışlarını nasıl etkilediği analiz edilmiştir. Çalışmanın sonuçları, uzmanlık alanlarında herhangi bir ayırım yapılmaksızın tüm çalışanların davranışlarının ve bilgi güvenliği eğitim programlarının iyileştirilmesine yardımcı olabilir. Amaca istinaden, detaylı bir literatür taraması çalışması yürütülmüş, araştırma modeli geliştirilmiştir. Anket birincil veri kaynağı olarak kullanılmıştır. Anket için soru geliştirmek üzere, literatür taraması dışında bilgi güvenliği uzmanlarının görüşlerine başvurulmuştur. Çevrimiçi anket Türkiye’de bulunan şirketlerde çalışan kişiler üzerinde yürütülmüştür. Alınan toplam 315 yanıt, bu çalışmada önerilen beş adet hipotezin test edilmesi için kullanılmıştır.

ACKNOWLEDGEMENTS

First of all, I would like to thank my thesis advisor, Assoc. Prof. Dr. Bilgin Metin for his continuous support, encouragement and confidence in me. Without his point of view, this would be just a “thesis” for me. I would also like to thank Assoc. Prof. Dr. Hande Türker for her support during my thesis especially developing the research model. I am really thankful to Assist. Prof. Dr. Tuğba Yıldız for her valuable comments about my thesis. I really appreciate Assoc. Prof. Dr. Sona Mardikyan and Assoc. Prof. Dr. Bertan Badur for their support and guidance in analysis part of thesis, Dr. Nazım Taşkın for his insightful comments and help.

I am very grateful to have an opportunity for having valuable opinions of Kaya Kazmirci, Mehmet Zeki Önal and İsmail Burak Tuğrul which improves my thesis work. I am also thankful to Büsiber’s young talents for their positive energy, knowledge and support. Also, I would like to thank my academic advisor Prof. Dr. Zuhâl Tanrıku for her care. I am also very thankful to Prof. Dr. Aslı Sencer for always giving me inspiration and courage.

I really appreciate to working with such an amazing team in PwC Turkey. I am really thankful to my managers for support, and especially Özkan Kıvanç for motivating me and believing in me during the whole process. I am very glad to have Kalaycı Family who is always supportive and excited for anything about me, and Mathematical Engineers in my life who are the source of morale. I cannot imagine a better groupmate than Merve Bilici, I am very thankful for all of the memories.

I am extremely lucky to have my parents, Mürüvvet Tanrıverdi and Hasan Tanrıverdi. I really appreciate to their endless care, love, patience and support during whole my life.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION	1
CHAPTER 2: LITERATURE REVIEW	4
2.1 Information security awareness and behavior studies.....	4
2.2 Familiarity concept in studies	15
CHAPTER 3: THEORETICAL MODEL AND HYPOTHESES	26
3.1 Theoretical model.....	26
3.2 Part 1: The effect of information security familiarity’s four focus areas on security incident awareness.....	27
3.3 Part 2: Effects of security incident awareness on security behavior	36
CHAPTER 4: METHODOLOGY	38
4.1 Data collection	38
4.2 Research instruments	39
CHAPTER 5: ANALYSES AND FINDINGS	54
5.1 Descriptive findings	54
5.2 Reliability and descriptive statistics of multi-item scale questions	60
5.3 Hypotheses tests	65
CHAPTER 6: DISCUSSION AND CONCLUSION	86
6.1 Discussion	86
6.2 Conclusion.....	92
6.3 Future studies	94
APPENDIX A: ENGLISH QUESTIONNAIRE.....	95
APPENDIX B: TURKISH QUESTIONNAIRE.....	102
APPENDIX C: DESCRIPTIVE STATISTICS	114
APPENDIX D: RELIABILITY TEST RESULTS	117

APPENDIX E: LINEARITY ASSUMPTION TEST RESULTS.....	119
APPENDIX F: MULTIPLE REGRESSION TEST RESULTS	121
APPENDIX G: DESCRIPTIVE STATISTICS OF 60 RESPONDENTS.....	125
APPENDIX H: WLS REGRESSION TEST RESULTS.....	129
APPENDIX I: ADDITIONAL ANALYSES: MULTIPLE REGRESSION TEST OF PART 1 AFTER EXCLUDING 60 RESPONSES.....	132
APPENDIX J: ADDITIONAL ANALYSES: PROFFESION DIFFERENCE WITH RESPECT TO THREAT KNOWLEDGE AND PROTECTION KNOWLEDGE	137
APPENDIX K: ADDITIONAL ANALYSES: GENDER DIFFERENCE WITH RESPECT TO SECURITY INCIDENT AWARENESS AND SECURITY BEHAVIOR	139
REFERENCES.....	141

LIST OF TABLES

Table 1. Familiarity Measurement Approaches in Existent Literature	16
Table 2. Summary of Variable Questions	41
Table 3. Protection Knowledge Measure	46
Table 4. Breach Experience Measure.....	48
Table 5. Protection Indicator Familiarity Questions	49
Table 6. Security Incident Awareness Measure	51
Table 7. Information Security Behavior Measure	52
Table 8. Demographic Profile of Respondents	55
Table 9. Company Information of Respondents	56
Table 10. Working Information of Respondents.....	57
Table 11. Technology Usage of Respondents.....	58
Table 12. Descriptive Statistics of Threat Knowledge, Breach Experience and Protection Indicator Familiarity Variables	59
Table 13. Reliability/Internal Consistency of Survey Items	61
Table 14. Mean Values of Protection Knowledge	62
Table 15. Mean Values of Security Incident Awareness	64
Table 16. Mean Values of Information Security Behavior	66
Table 17. Spearman's Rank Correlation Test Results.....	70
Table 18. Tolerance and VIF Values of Variables.....	71
Table 19. Summary of Multiple Regression Analysis	74
Table 20. Excluded Variables of Regression Model.....	74
Table 21. Summary of Multiple Regression Analysis	83

LIST OF APPENDIX TABLES

Table C 1. Descriptive Statistics of First Threat Knowledge Question	114
Table C 2. Descriptive Statistics of Second and Third Threat Knowledge Question	114
Table C 3. Descriptive Statistics of Breach Experience	115
Table C 4. Descriptive Statistics of Protection Indicator Familiarity	116
Table D 1. Reliability Statistics of Protection Knowledge	117
Table D 2. Item-Total Statistics of Protection Knowledge	117
Table D 3. Reliability Statistics of Security Incident Awareness	117
Table D 4. Item-Total Statistics of Security Incident Awareness	118
Table D 5. Reliability Statistics of Information Security Behavior	118
Table D 6. Item-Total Statistics of Information Security Behavior	118
Table F 1. Descriptive Statistics	121
Table F 2. Model Summary ^c	121
Table F 3. ANOVA ^a	121
Table F 4. Correlations	122
Table F 5. Coefficients ^a	123
Table F 6. Excluded Variables ^a	124
Table G 1. Demographics of 60 Respondents	125
Table G 2. Company Information of 60 Respondents	126
Table G 3. Working Information of 60 Respondents	127
Table G 4. Technology Usage of 60 Respondents	127
Table G 5. Descriptive Statistics of Security Behavior	128
Table H 1. Descriptive Statistics ^a	129

Table H 2. Correlations ^a	129
Table H 3. Variables Entered/Removed ^{a,b}	129
Table H 4. Model Summary ^{b,c}	129
Table H 5. ANOVA ^{a,b}	130
Table H 6. Collinearity Diagnostics ^{a,b}	130
Table H 7. Coefficients ^{a,b}	131
Table H 8. Residual Statistics ^{a,b}	131
Table I 1. Descriptive Statistics	132
Table I 2. Correlations.....	133
Table I 3. Model Summary ^d	134
Table I 4. ANOVA ^a	134
Table I 5. Coefficients ^a	135
Table I 6. Excluded Variables ^a	136
Table J 1. Group Statistics	137
Table J 2. Independent Samples Test.....	137
Table J 3. Group Statistics	138
Table J 4. Independent Samples Test.....	138
Table K 1. Group Statistics	139
Table K 2. Independent Samples Test.....	139
Table K 3. Group Statistics	140
Table K 4. Independent Samples Test.....	140

LIST OF FIGURES

Figure 1. Focus areas and sub-areas of information security policies	7
Figure 2. Theories and constructs in theory based studies.....	9
Figure 3. Information security conceptual model	10
Figure 4. Level of familiarity of web sites.....	17
Figure 5. Common threats of information security based on categories.....	20
Figure 6. Security technology awareness rates	20
Figure 7. Different end-users profiles based on activities and experiences.....	23
Figure 8. Effects of familiarity on login behavior.....	24
Figure 9. Theoretical model	27
Figure 10. Answers of “were your company's systems attacked by an outsider in the last year?” classified by professions of employees.....	29
Figure 11. Scatterplot of studentized residual against unstandardized predicted value	69
Figure 12. Distribution of residuals	72
Figure 13. P-P plot of residuals.....	72
Figure 14. Scatterplot of security behavior against security incident awareness.....	76
Figure 15. Scatterplot of security behavior against security incident awareness.....	79
Figure 16. Scatterplot of residual of the model against security incident awareness	80
Figure 17. Scatterplot of weighted residual value against weighted predicted value	81
Figure 18. Distribution of weighted residuals of WLS regression	81
Figure 19. P-P plot of weighted residuals of WLS regression.....	82

LIST OF APPENDIX FIGURES

Figure E 1. Linearity check for threat knowledge.....	119
Figure E 2. Linearity check for protection knowledge	119
Figure E 3. Linearity check for breach experience	120
Figure E 4. Linearity check for protection indicator familiarity.....	120

CHAPTER 1

INTRODUCTION

Main concern of both theory and practice is finding more sophisticated and effective solutions to protect corporate data and information systems against to advanced security threats. In practice, by the help of such disciplines as machine learning and artificial intelligence, security technology is continuously improved to protect systems better. Security systems become more useful, robust and smarter in order to protect information systems in more sophisticated way. In today's world, laws and regulations are developing, such as European Union General Data Protection Regulation (Eugdpr.org, n.d.) and Turkish Personal Data Protection Law (KVKK, 2016) so as to constitute a base for risky security environment.

On the other hand, in recent studies researchers investigate different dimensions of security, they all have one aim which brings better protection. One of the main focuses of these studies is people. Because of that people involve information systems and they are part of information oriented world at the end. Their behavior in a work place which has a great potential to threat information systems is main focus of studies in this area. In order to understand behavior of people, there are various approaches which have been measured in different levels, such as organizational, individual and socio-environmental (Haeussinger & Kranz, 2017; Jaeger, Ament, & Eckhardt, 2017). Understanding the human factor in information security is one of the most important approach to change people's behavior and security awareness. Factors which have an effect on behavior and/or information security awareness of people are usually investigated to improve security habit, behavior and awareness level of them. Even generational differences between

people, such as difference between millennials and baby boomers, are studied (Cummings, Gomillion, & Connolly, 2017; Tanriverdi & Metin, 2017a) in order to improve their security behavior and awareness level.

These developments become more important in digital transformation. According to results of information security survey conducted globally by PricewaterhouseCoopers (PwC), 63 percentage of respondents claimed that their companies run their information technology (IT) function in the cloud. The 36 percentage of respondents are running their operation function in the cloud, while the percentage of customer service is 36, market and sales is 34 and finance function is 32 in the cloud (2016). With the effect of digitalization, information security becomes more and more important. According to 59 percentage of respondents of global information security survey, digitalization leads companies to increase spending on security. Additionally, people become more involved the information oriented world and more integrated with information security systems. Thus, skills of employees should be adapted to the new conditions.

In this study, whether employees are capable to be a part of information security protection in their companies is investigated. With this purpose, study begins with measuring the effect of information security familiarity on security incident awareness, then how security incident awareness affects security behavior is attempted to analyze. Implications of this study can help to improve employees' behavior without any distinction between professions as well as information security awareness education and training programs.

Information security familiarity is evaluated with considering both knowledge and experience of employees in four focus areas; threat knowledge, protection knowledge, breach experience and protection indicator familiarity. Information

security familiarity can be considered as an extension of IT/non-IT profession approach which has been researched in prior study (Tanriverdi & Metin, 2017b). The most important result of the study is that knowledge about insider related security incidents are not dependent on whether employees' professions are IT related or non-IT related, whereas knowledge about outsider related security issues depend on professions. To investigate information security familiarity as the common point of IT people and non-IT people who know insider/outsider security incidents of their companies is triggered by the result of Tanriverdi and Metin's study.

In order to achieve the purpose of this study, detailed literature review has been conducted and research model has been developed based on the literature review. Primary data source of this study is a survey. In order to develop questions for the survey, security experts' opinion has been consulted. An online survey has been conducted on employees who works in companies located in Turkey. Totally 315 responses have been used to conduct analyses which have been applied to test five hypotheses proposed in this study.

This paper is organized as follows; Chapter 1 introduces study generally. In Chapter 2 related literature on security behavior and awareness, and familiarity concept in security context is summarized. In Chapter 3, research model, basis of the model, variables, and proposed hypotheses of this study are given. In Chapter 4, how primary data is collected for this study is summarized, then measurement methods of variables are provided. Conducted hypotheses test results, main findings and additional test results are shown in Chapter 5. Important findings are criticized, main findings and contribution of this study, and future research is provided in Chapter 6.

CHAPTER 2

LITERATURE REVIEW

In this chapter, according to the main focus of this thesis, related studies in literature is reviewed. How security behavior and security awareness concepts have been evaluated is examined within the literature review in order to show the usage of these concepts broadly. It is seen from the literature that security behavior and awareness have been studied many times. In some studies, different theories are used to explain security behavior and its factors. There are many investigated factors of security behavior in studies. However, how literature studies have used security awareness is examined in this chapter. Factors of security awareness is also evaluated. It is understood from the literature that different factors of security awareness have been analyzed in different aspects. Individual aspects including knowledge and experience factors, which are more related to this thesis, are examined.

Besides information security awareness and behavior studies, in order to enhance profession approach to information security familiarity, familiarity concept is reviewed in literature. Definition of familiarity, scale of familiarity measure and findings related to familiarity are reviewed in existent literature.

2.1 Information security awareness and behavior studies

Existent literature shows that relationship between information security behavior and information security awareness have been investigated many times. There are also some studies which review existed literature systematically and extensively, and summarize what have been done related to information security behavior and awareness (Abraham, 2011; Lebek, Uffen, Neumann, Hohler and Breitner, 2014).

2.1.1 Applied theories in literature

A theory-based literature review study has been conducted by Lebek et al. (2014).

This literature review study collects theory-based information security awareness and behavior studies (Lebek et al., 2014). They have summarized which theories have been investigated in information security literature, which constructs have been studied, how many times they have been studied and how methodology of studies have been designed in studies which have been published before 2014.

According to Lebek et al. (2014)'s study, although they identified 54 different theories in the literature, 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). They have also claimed that these theories have been adapted to information security area from different disciplines, such as psychology, sociology and criminology. Besides investigating a single theory, some combinations of the theories have been researched to fulfill the gap in the literature (Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009; Ifinedo, 2012; Herath et al., 2012; Hu and Dinev, 2007; Pahnla, Siponen, & Mahmood, 2007; Siponen, Pahnla, & Mahmood, 2007; Siponen, Pahnla, & Mahmood, 2010). Lebek et al. (2014) summarized that aforementioned theories have explained security behavior of employees with investigating various related factors.

2.1.2 Security behavior related constructs

In order to measure security behavior of people there are different approaches in literature studies. Those are actual behavior and behavioral intention as it is seen in literature.

2.1.2.1 Actual security behavior

Security behavior, mostly named actual behavior in literature, has been measured with frequency of behavior (Limanyem & Hirt, 2003; Siponen et al. 2007). In these studies participants' responses have been collected with survey. They have been directly asked to declare what is the frequency of their security behavior. Security behavior has been also considered as behavior complying with information security policy of company in the literature (Pahnila et al., 2007; Siponen et al., 2010).

Security policy compliance behavior has been measured with a self-reported question in Siponen et al.'s studies (2010).

Besides these theories which have measured actual behavior with self-reported questions, there are some studies which have evaluated security behavior with asking participants whether they are doing certain behavior (Ng, Kankanhalli, & Xu, 2009; Parson, McCormac, Butavicius, Pattinson, & Jerram, 2014; Rhee, Kim, & Ryu, 2009). Parson et al. (2014) have been evaluated security behavior with seven focus areas. They have determined seven focus areas with three subareas based on the review of many information security policies and interview with security managers given in Figure 1. They have evaluated security behavior in agreement scale. Ng et al. (2009) have measured security behavior in the email service usage context with using agreement scale. Rhee et al. (2009) have measured security behavior in two dimensions; technology aspect and security conscious care behavior.

With technology aspect question, employees' practice related to security technology usage mainly on software, such as antivirus, antispymware, firewall and even blocking function of pop-up window and spam filtering function have been asked. In the second question of information security practice, they have evaluated how they are using computer and Internet in terms of security conscious care. For instance, using strong password, file sharing software, having backup of data and files etc. have been included in the measure. They have claimed that they have developed these measures based on published security guidelines and security providers' advices.

Focus area	Sub-areas
Password management	Locking workstations Password sharing Choosing a good password
Email use	Forwarding emails Opening attachments IT department level of responsibility
Internet use	Installing unauthorised software Accessing dubious websites Inappropriate use of internet
Social networking site (SNS) use	Amount of work time spent on SNS Consequences of SNS Posting about work on SNS
Incident reporting	Reporting suspicious individuals Reporting bad behaviour by colleagues Reporting all security incidents
Mobile computing	Physically securing personal electronic devices Sending sensitive information via mobile networks Checking work email via free network
Information handling	Disposing of sensitive documents Inserting DVDs/USB devices Leaving sensitive material unsecured

Figure 1. Focus areas and sub-areas of information security policies

Source: (Parson et al., 2014)

2.1.2.2 Behavior intention

Lebek et al. (2014) have also revealed that behavior intention has been evaluated within theories. Behavior intention has been defined as one's belief or plan to act

certain behavior some day (Bulgurcu et al., 2010; Hu, Dinev, Hart, & Cooke, 2012; Johnston, Warkentin, & Siponen, 2015). Behavior intention has been measured with participants' declaration about their intention and likelihood to keep security complied behavior in the future in several studies (Al-Omari, El-Gayar, Deokar, 2012; Bulgurcu et al., 2010; Haeussinger & Kranz, 2013; Herath & Rao, 2009; Hu et al., 2012; Ifinedo, 2012; Siponen et al., 2010). Additionally, Hu and Dinev (2007) have measured behavior intention with intention of participants to apply protective methods against to spyware. Hovav and D'Arcy (2012) who conducted a case study have assessed behavior intention by self-reported likelihood of sending an e-mail at the certain case. Limanyem and Hirt (2003) have evaluated frequency of intention to use certain web site (WebBoard) to measure behavior intention. Reason of using behavior intention instead of actual behavior is that measuring of actual behavior is complicated for researchers according to Vroom and von Solms (as cited in Lebek et al., 2014, p. 1054). Information security researches have proven that there is a strong relationship between behavioral intention and actual behavior in several studies (Limanyem & Hirt, 2003; Pahnla et al., 2007; Siponen et al. 2007; Siponen et al., 2010).

2.1.3 Factors of security behavior

Lebek et al. (2014) have summarized in their study that under four most frequent theories 11 different independent variables have been investigated to predict actual behavior and behavior intention given in Figure 2. Lebek et al. (2014) have claimed that there are also some studied factors which have not based on any theories, such as awareness, perceived awareness and organizational commitment.

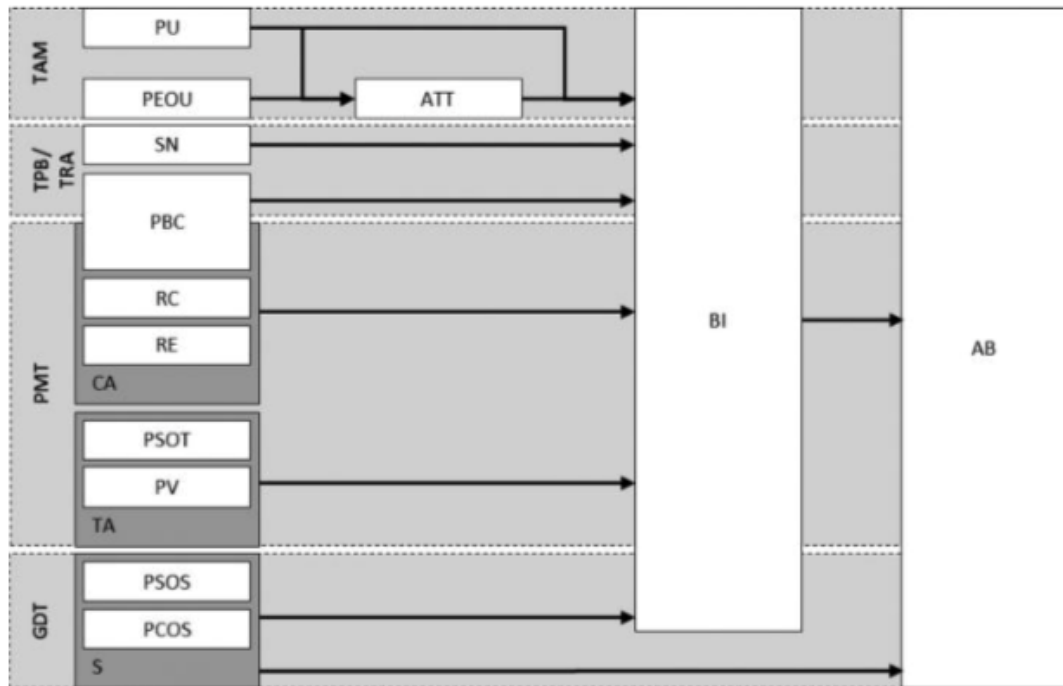


Figure 2. Theories and constructs in theory based studies

Source: (Lebek et al., 2014)

Note: PU: perceived usefulness, PEOU: perceived ease-of-use, ATT: attitude toward information security, SN: subjective norm, PBC: perceived behavioral control, RC: response cost, RE: response efficacy, CA: coping appraisal, PSOT: perceived severity of threats, PV: perceived vulnerability, TA: threat appraisal, PSOS: perceived severity of sanctions, PCOS: perceived severity of sanctions, S: self-efficacy, BI: behavioral intention, AB: actual behavior

Abraham (2011) has also investigated factors which have an effect on information security behavior are summarized in the study. It has been identified in the study that 18 different concepts have been investigated in information security behavior studies as effective factors on information security behavior (Abraham, 2011). While investigating studied factors in literature, Leach's "information security conceptual model" has been adapted. In Leach's model given in Figure 3, there are six main

categories that enable to understand the context of studies. Model proposes not only intrinsic factors like user's psychology, personal values or decision making skills, but also extrinsic factors, such as security procedures or policies (the body of knowledge).

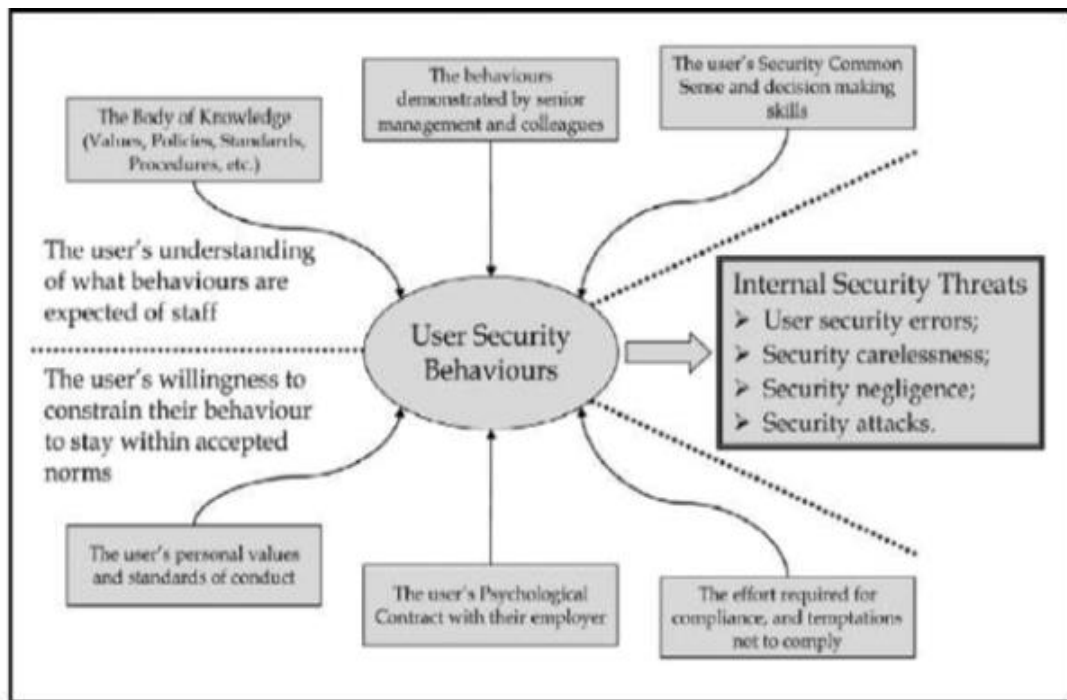


Figure 3. Information security conceptual model

Source: Leach's information security conceptual model (as cited in Abraham, 2011, p. 3)

2.1.4 Security awareness as a factor of security behavior

It is seen from information security literature that awareness is one of the most important factors to predict security behavior and at the same time as a concept it is approached differently.

As Lebek et al. (2014) have shown in their study that security awareness is one of the major concepts having an influence on information security behavior.

Even if security awareness is conceptualized and measured differently in studies (Bulgurcu et al., 2010), it is understood that the main approach is mostly same. Security awareness is being aware, knowledgeable, conscious and recognizant in terms of security risks, objectives, responsibilities and protective methods against to threats (Haeussinger & Kranz, 2017).

Bulgurcu et al. (2010) have depicted general awareness and information security policy awareness as information security awareness. In their study, general awareness has been evaluated with understanding threats, risks and possible results of security incidents. Haeussinger, and Kranz (2013) have used same security awareness measure as Bulgurcu et al. performed. Johnston, Wech, Jack, & Beavers (2010) have also approached awareness with being aware of information security policy of company. What is more, Hu and Dinev (2007) have adapted awareness in the context of technology. They have defined technology awareness as “user’s raised consciousness of and interest in knowing about technological issues and strategies to deal with them” (Hu & Dinev, 2007, p. 402). Ryan (2007) has evaluated security awareness as a combination of technology perception, policy perception and threat-context perception. Author has considered technology perception with users’ knowledge on how antivirus applications and firewall systems protect information systems. Policy perception has included items regarding awareness of research participants about what policy dictates and requires for protection in the organization. Lastly, awareness of current possible threats and protection methods against to threats has reflected threat-context perception. Zhang and Li (2015) have designed different approach in their research in progress paper that classification of information security awareness has been performed. They have haven two category of security awareness as perceived and assessed awareness. AlKalbani, Deng, and

Kam (2015) have assessed information security awareness as a component of information security culture.

Authors have provided their security measures and scales in their studies, even if some of studies do not include measures of security awareness (AlKalbani et al. 2015; Johnston et al., 2010; Zhang & Li, 2015). It is seen from those measures that most of studies have developed measure as self-reported question. Security awareness has been measured with participants' self-evaluation about their awareness level in Likert-type scale in these studies (Bulgurcu et al., 2010; Haeussinger, Kranz, 2013; Ryan, 2007). Only Hu and Dinev (2007) have been differently evaluated security awareness. They have asked technological strategies in order to measure technology awareness agreement scale (Hu & Dinev, 2007).

It is understood from the results of these studies that, Johnston et al. (2010) have discovered the effect of awareness of information security policy on behavior intention. Hu and Dinev (2007) have also figured out that technology awareness has an influence on the intention of using of security protection technology. However, Bulgurcu et al. (2010) have not investigated the relationship between information security policy awareness, and behavior intention or actual behavior. They have found that security awareness changes employees' attitude toward information security policy compliance. Haeussinger, and Kranz (2013) have found the effect of security awareness on intention to comply with security policy. Even if, AlKalbani et al. (2015) have not specified how they measured information security awareness of employees, they have found that information security compliance has been influenced by security awareness.

2.1.4.1 Factors of security awareness

In some studies factors which have an effect on security awareness have been investigated. Haeussinger and Kranz (2017) have identified factors which are used to define and measure security awareness. They have conducted a literature review and provided antecedents of information security awareness in their work. They have classified studied factors of information security awareness into three categories. Institutional, individual and socio-environmental factors of information security awareness are summarized in their work. Jaeger et al. (2017) have also grouped antecedents of security awareness. They have identified same categories with Haeussinger and Kranz's study (2017). Besides they have identified technological antecedents of awareness which includes just in time reminders and security warnings as well.

Institutional level factors of information security awareness are based on security management applications of organization (Haeussinger & Krams, 2017). Firm-wide conducted practices are the focus of the factors in this category. At first, security awareness of management is evaluated as antecedent of information security awareness. Management is expected to be aware of information security risks and threats. Then security is leaded, supported and promoted by managerial level, this is another criteria of organizational security awareness. Additionally, organization' information security policy is considered important institutional factor to determine security awareness. Information security education training and awareness (SETA) programs are also evaluated under institutional level factors. Active participation of all employees to information security protection and maintenance is important as well as leadership of management level according to them. Thus, support of employees to develop SETA programs is seen an organizational level factor.

Socio-environmental antecedents are other category that authors have been determined factors of security awareness related to people's social environment. Socio-environmental factors affect security awareness according to them. Employees interact with not only people like their peers and stakeholders, but also external resources, such as mass media, news, security journals, and public awareness. These factors have been identified as socio-environmental antecedents.

Haeussinger and Kranz (2017) have determined individual level factors coming from employees as an entity of information security system in studies. Information system knowledge and literacy, negative experience with information security threats, personal education and security perception have been identified as individual level factors. Individual factors are more related to the scope of this thesis, thus these individual factors from studies are analyzed in detail. It can be understood that knowledge and experience are commonly studied individual antecedents of security awareness. Experience has been evaluated with direct or indirect negative experience in studies.

One of them has been conducted by Johnston et al. (2010) who have been investigated "situational support", "verbal persuasion" and "vicarious experience" as a factor of security awareness. They have found that vicarious experience significantly influences security awareness, whereas situational support and verbal persuasion do not. Based on their definition, vicarious experience is what people experienced indirectly by observation. Moreover, Haeussinger and Kranz (2013) have assess employees' direct negative experiences with asking them whether they have ever haven virus or spyware in their systems. They have found positive effect of experiences on security awareness. Zhang and Li (2015) have designed a model which says experiences have an influence on both perceived and assessed security

awareness. According to their experience definition they have developed experience measure which asks the number of information security incidents research participants have. Additionally, Bulgurcu et al. have stated that “life experiences, such as having once been harmed by a virus attack or penalized for not adhering to security rules and regulations may increase an individual’s information security awareness” (as cited in Haeussinger & Kranz, 2013, p. 4). General information security knowledge which has been measured with self-evaluation of general computer, Internet and e-mail service knowledge has found as effective factor of security awareness (Haeussinger & Kranz, 2013).

2.2 Familiarity concept in studies

First of all, familiarity concept has been evaluated in related studies with the aim of determining the boundaries and measurement methods of familiarity concept for this study. These studies can be divided into two groups, IT related and information security related, based on the context of familiarity. Moreover, it can be seen that familiarity with IT/information security has been measured with self-reporting familiarity level, or other Likert, numerical or nominal scale question based on familiarity definition of the study. Studies have been summarized in Table 1.

2.2.1 Familiarity with IT

In IT related familiarity measurements, it can be understood from studies that familiarity has been mostly considered as being familiar with certain technology, web sites or online platforms (Heartfield, Loukas, & Gan, 2016; Kelley & Bertenthal, 2016; Pattinson, Jerram, Parsons, McCormac, & Butavicius, 2012; Rhee et al., 2009; Yang, Ng, & Vishwanath, 2015).

Table 1. Familiarity Measurement Approaches in Existent Literature

Familiarity Definition	Context	Measurement Method	References
Familiarity with platforms (Social media, email, public wifi, web browser, e-commerce)	IT related	Familiarity Scale	(Heartfield, Loukas, & Gan, 2016)
Familiarity with web sites (Amazon, Paypal, Netflix, eBay, Walmart, Reddit etc.)	IT related	Familiarity Scale	(Kelley, & Bertenthal, 2016)
Familiarity with computers	IT related	Frequency of usage	(Pattinson, Jerram, Parsons, McCormac, & Butavicius, 2012)
Familiarity with platforms (social media)	IT related	Familiarity Scale	(Yang, Ng, & Vishwanath, 2015)
Computer and Internet Experience	IT related	Years of using computer and Internet, Internet literacy level	(Rhee et al., 2009)
Breach Experience	Information security related	Nominal scale	(Rhee et al., 2009)
Familiarity with policies and procedures	Information security related	Not defined	(Luciano, Mahmood, & Maçada, 2010)
Familiarity with threats	Information security related	Familiarity scale	(Huang, Rau, & Salvendy, 2007)
Familiarity with security technology	Information security related	Awareness scale	(Furnell, & Karweni, 1999)
Familiarity with online threats	Information security related	Ranking of online threats	(Jeske, & Schaik, 2017)
Familiarity with mobile phone communication and safety security measures	Information security related	Familiarity scale	(Lomo-David, & Shannon, 2009)
Security familiarity	Information security related	Familiarity scale	(Ng et al., 2009)
Technical controls	Information security related	Agreement scale	(Ng et al., 2009)
Knowledge about Information security policy	Information security related	Agreement scale	(Parson et al., 2014)

For example, familiarity with platform has been measured in Heartfield et al.' study (2016). To measure familiarity with platforms comprehensively various platform types are involved, such as social media, email, public wifi, web browser and e-commerce in their study. Kelley and Bertenthal (2016) have been evaluated familiarity of the websites with certain web sites; Amazon, Paypal, Netflix, eBay, Walmart, Reddit etc. (see in Figure 4). Yang et al. (2015) have also approached familiarity as a knowledge about online social media sites. Social media familiarity

can be developed by using social media sites and gaining information from other users or other sources according to authors. In these studies, familiarity has been measured with self-reporting questions. Survey has been conducted and the surveys participants have been asked to evaluate themselves about how much they are familiar with specific subject. 3 or 5 point numerical scale has been used to measure familiarity level, such as “not at all familiar”, “slightly familiar”, “somewhat familiar”, “moderately familiar”, “extremely familiar” in these studies.

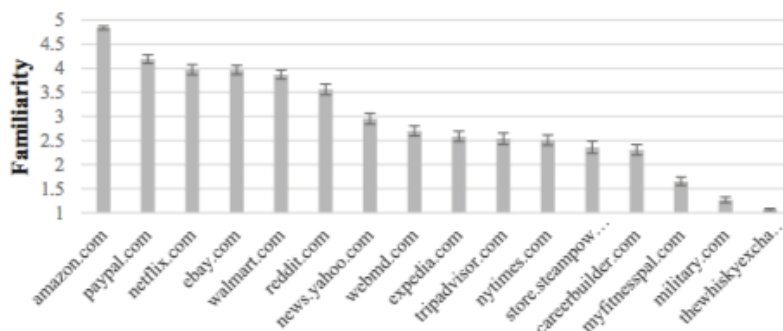


Figure 4. Level of familiarity of web sites

Source: (Kelley & Bertenthal, 2016)

Familiarity has been measured in Pattinson et al.’s study (2012) as familiarity with computers. Computer familiarity measure has included various aspects regarding frequency of accessing computer, internet, and email services from different environments, such as home, work, university, other public computers or other private computers. Using applications like Paypal, eBay, Facebook, MySpace, Twitter and online purchasing, and doing such activities as e-mailing, web surfing, researching, word processing and playing games have also been taken account into consideration. Rhee et al. (2009) have evaluated computer and Internet experience in their study with how many years they have used computer and Internet. Even if they

have not named the concept as “familiarity”, it can be assessed as familiarity. It can be understood that their measurement method for familiarity is different from self-reported familiarity level approach.

2.2.2 Familiarity with information security

Additionally, in some studies familiarity has been measured directly in information security context. For example, it has been considered being familiar with security technologies and measurements in various studies (Furnell, & Karweni, 1999; Lomo-David, & Shannon, 2009; Ng, Kankanhalli, & Xu, 2009; Parson et al., 2014) or threats (Huang, Rau, & Salvendy, 2007; Jeske & Schaik, 2017; Rhee et al., 2009).

Lomo-David and Shannon (2009) have asked participants to evaluate themselves that how familiar they are with information security and safety methods in their study. They have included totally eight security measures as a “mobile phone communication devices” protection method; passwords, daily system scan, scan of email attachments, anti-virus software, passwords on email attachments, biometric authentication, firewalls, multifaceted authentication systems. Furnell and Karweni (1999) have associated awareness of security technologies to familiarity with security technologies as well. Security technologies, such as data encryption standard, digital/electronic signature, certification authority, secure electronic transaction and trusted third party have been asked to survey participants to assess their familiarity with security protection technologies in their study. Ng et al. (2009) have evaluated security familiarity and technical controls. Participants have been asked to rate their familiarity with applications on computer security in order to measure security familiarity. In technical control construct whether participants’ companies apply antivirus protection is asked to them. Parson et al. (2014) have

measured information security policy knowledge of employees in seven focus areas with three most important subareas (given in Figure 1) to represent common points of information security policy. They have asked to participants whether they know the issue specified in policy.

Jeske and Schaik (2017) measured familiarity with online threats which have been grouped into two; newer and well-known threats. Cat-fishing, social engineering, email harvesting, zero-day attack, rogueware, botnet, trojan, keylogger, phishing has been labeled as newer threats, whereas well-known threats have been given with spyware, cyber-bullying, virtual stalking, internet surveillance, identity theft, cookie. They have directly given definition of these threats and asked participants to rank whether they are familiar with the definition. Similarly, Huang et al. (2007) have approached familiarity as how people know threats then how they feel themselves about threats. They have measured familiarity with threats that include common 21 threats under 12 categories given in Figure 5. As a different approach of threats, Rhee et al. (2009) have been evaluated breach experience whether employees had ever security incidents, such as virus, spyware and cyber fraud.

Besides knowledge, experience and Internet usage frequency, awareness has been associated with familiarity (Furnell & Karweni, 2009). Because they have inferred that there is inconsistency between given answers for security technology awareness provided in Figure 6, they have claimed that respondents have misinterpreted given security technologies. Also, familiarity with policies and procedures has been evaluated as human factors of information security (Luciano, Mahmood, & Maçada, 2010).

Categories	Threats
1. Acts of human error or failure	Operation accidents
2. Compromises to intellectual property	Piratical software
3. Deliberate acts of espionage or trespass	Hacker Passwords attack Information wiretapping Users' online behaviors being recorded
4. Deliberate acts of information extortion	Data extortion
5. Deliberate acts of sabotage or vandalism	Denial-of-service(Dos)
6. Deliberate acts of theft	Computer theft Phishing
7. Deliberate software attacks	Virus Worms Trojan horse Backdoor Zombie PC SPAM
8. Forces of nature	Nature disaster (such as fire, earthquake, and lightning)
9. Deviations in quality of service	Deviation in quality of service from service providers
10. Technical hardware failures or errors	Hardware failure
11. Technical software failures or errors	Scampish software
12. Technological obsolescence	Software bugs

Figure 5. Common threats of information security based on categories

Source: (Huang et al., 2007)

Security technology	Aware respondents (%)
Data encryption standard (DES)	80
Digital/electronic signature	64
Certification authority (CA)	50
Secure electronic transaction (SET)	42
Trusted third party (TTP)	33

Figure 6. Security technology awareness rates

Source: (Furnell & Karweni, 2009)

2.2.3 Findings related to familiarity

Besides definitions and scales of familiarity measure, studies have common points according to research purposes and findings. Therefore, familiarity can be evaluated

in three main groups;

- i. Extracting factors which affect familiarity,
- ii. Evaluating familiarity as a component of any concept,
- iii. Testing whether familiarity has a significant effect on a variable

It has been seen in some studies that they have helped to understand familiarity conceptually in information security context. Knowledge, experience and Internet usage frequency are common points of those studies that have been associated with familiarity. However, research perspective and how researchers built relationship between experience, knowledge, Internet usage frequency, and familiarity concepts are differed.

Some studies have revealed that familiarity is a component (Huang et al., 2007; Luciano et al., 2010; Nishioka, Murayama, & Fujihara, 2012), while others have found factors which have an effect on familiarity (Furnell & Karweni, 1999; Jeske & Schaik, 2017; Lomo-David & Shannon, 2009; Yang et al., 2015).

Huang et al. (2007) have evaluated that familiarity is one of the component of knowledge. They have approached familiarity with how people know threats then how they feel themselves about threats. If a threat is new and they do not know so much about the threat, they do not feel familiar with the threat based on their results. In order to do this, they have modelled factors which affect people's information security perceptions on threats. At the end of the work, related factors have been grouped together. Results show that those groups have been determined as knowledge, impact, severity and possibility. Lomo-David and Shannon (2009) have emphasized both knowledge and experience that if respondents have a knowledge and experience with mobile devices they are more familiar with four mobile phone

security protection methods; password usage, scan of e-mail attachments, antivirus software usage, password usage on e-mail attachments. Nishioka et al. (2012) have also considered familiarity concept as feeling familiar with the service based on what they have practiced by themselves and impressed from another users' practice. They have studied on users' "anshin" which means "sense of security" in Japanese in their research. They have created a survey which includes 937 subjects in order to find factors of "anshin". In their study, they have subjected users who do not have technical knowledge. They have found that cognitive trust, familiarity and reputation are subjective factors of "anshin". Similar to Nishioka et al.'s approach, Yang et al., (2015) have mentioned users' own practice and what they know from media or other users' experience can change knowledge about social media which social media familiarity relates with. They have also claimed that internet usage frequency can change familiarity with social media. Internet usage frequency has been also evaluated with "how long they have been using internet", "how often they log onto internet", "how much time spend on internet per day" questions in Jeske and Schaik's study (2017). Experience has been used for user profiling in terms of security in Rughiniş and Rughiniş's study (2014). They have categorized European Union end users given in Figure 7 based on their online activities and experiences regarding daily Internet usage, variety of online activities, security incident experiences and protection methods (using antivirus software, multiple passwords, changing passwords, visiting trusted websites, and opening emails from people they know).

Furthermore, familiarity has been measured as a construct to test hypotheses which propose whether familiarity affects other variables (Heartfield et al., 2016; Jeske & Schaik, 2017; Kelley & Bertenthal, 2016; Lomo-David & Shannon, 2009;

Ng et al. 2009; Parson et al., 2014; Pattinson, et al., 2012; Rhee et al., 2009; Yang et al., 2015).



Figure 7. Different end-users profiles based on activities and experiences

Source: (Rughiniş & Rughiniş, 2014)

In some studies effects of familiarity on behavior is investigated. Lomo-David and Shannon (2009) has researched in their study that whether there is a significant relationship between familiarity with mobile phone security protection methods and application of same methods in real life. According to results of their study, student's familiarity with three of mobile phone security measures are significantly related with how they apply these measures in actual usage. These three mobile phone security measures are scan of e-mail attachments, anti-virus software and biometric authentication. They have concluded that students have applied security protection measures which they are familiar with.

Moreover, it has been found that people better manage phishing emails when they are more familiar with computers according to Pattinson et al. (2012). However, they have mentioned that their result is valid while they inform participants about

their involvement to phishing study. Kelley and Bertenthal (2016) have investigated how their familiarity with web sites, such as Amazon, Paypal, Netflix, eBay, Walmart, Reddit etc. affect their decision to login to these websites. They have designed an experiment with manipulating web sites to test participants' login decisions. They have shown that familiarity provides people better recognize manipulation on web sites. As it is given in Figure 8, probability of login action in no-spoofed web sites is better than in spoofed web sites.

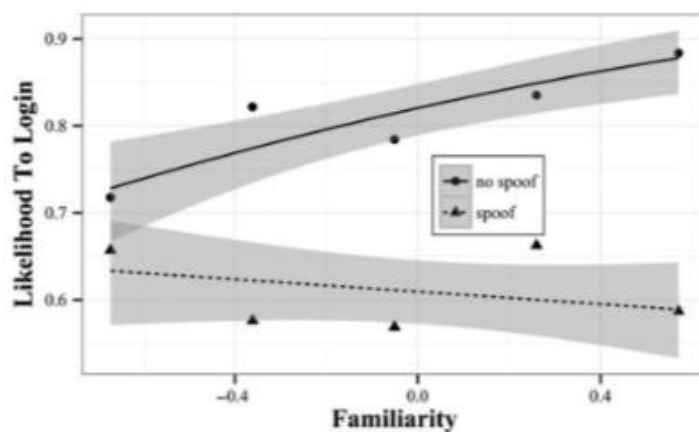


Figure 8. Effects of familiarity on login behavior

Source: (Kelley & Bertenthal, 2016)

Additionally, Jeske and Schaik (2017) have provided that familiarity significantly predict computer security behavior. Yang et al., (2015) have analyzed whether familiarity with social media sites leads to agree with privacy policy of social media sites. They have chosen Facebook because of the possible familiarity of people, and Cyworld in unfamiliarity direction. According to the results their study if people are familiar with social media sites, they better evaluate privacy policy of those sites. Moreover, in their study, they have concluded that people trusts their social media familiarity rather than privacy seals in terms of privacy concerns like judging privacy

policy about the social media platform (Yang et al., 2015).

On the other hand, there are also some findings about the side effects of familiarity in these studies (Heartfield et al., 2016; Kelley & Bertenthal, 2016; Yang et al., 2015). According to Heartfield et al. (2016), familiarity with a specific platform makes people less susceptible to social engineering attacks. Yang et al. (2015) have also found in their study that people tend to less care privacy policies in the social media sites when they are familiar with those sites besides positive effects of familiarity. Kelley and Bertenthal (2016) have determined negative consequences of familiarity in addition to positive results. They have claimed that when people are familiar with a web site, they tend to pay less attention to signs related to security. Reason of this situation is mainly habits according to them.

However, Ng et al. (2009) have proposed security familiarity and technical controls as control variable of a research model that aims to extract factors of security behavior, because of aforementioned negative effect of familiarity with technology on security. According to their results security familiarity and technical controls have not influence the result.

Rhee et al. (2009) have not tested effect of breach experience, and computer and Internet experience directly on security behavior of employees. They have found that information security self-efficacy which has an effect on security behavior is influenced by breach experience, and computer and internet experience.

CHAPTER 3

THEORETICAL MODEL AND HYPOTHESES

3.1 Theoretical model

In this chapter, proposed research model of the study is explained. As it is seen in Figure 9, the model includes two parts in itself to understand and interpret the results. This model is developed based on existent studies in literature.

The first part of the model aims to focus on information security familiarity as an antecedent of security incident awareness. At the same time to expand the profession approach which has been studied in prior study (Tanriverdi & Metin, 2017). Information security familiarity is handled with four focus areas differently from literature studies which have used familiarity concept in the context of security. These focus areas, threat knowledge, protection knowledge, breach experience and protection indicator familiarity, are chosen in the light of literature review and tried to explain whether they have an effect on security incident awareness. As it is seen in literature given in Chapter 2 chosen focus areas of information security familiarity of this study to explain security incident awareness are combination of security awareness' antecedents which have been investigated in literature.

In the second part of the model whether security incident awareness has an effect on security behavior is investigated. Even if the effect of security awareness on security behavior has been studies in literature, security awareness is tried to be evaluated in the context of incidents and its effect on security behavior is analyzed in this study. In following sub-sections, part 1 and part 2 are explained in detail.

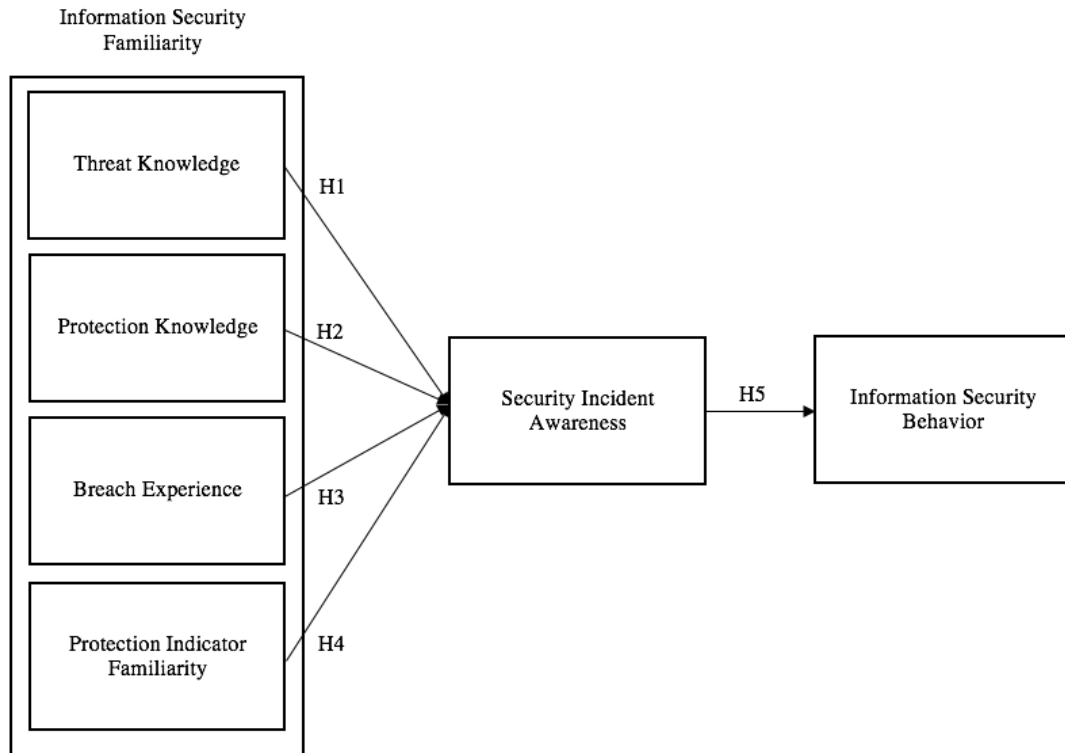


Figure 9. Theoretical model

3.2 Part 1: The effect of information security familiarity’s four focus areas on security incident awareness

In this part of the model, the effect of information security familiarity’s four focus areas, threat knowledge, protection knowledge, breach experience and protection indicator familiarity, on security incident awareness are examined. At the same time, this part of the study is constituted based on the most important finding of the study which has been conducted by Tanriverdi and Metin (2017). The study is summarized in following sub-section.

3.2.1 Basis of part 1: Evaluation of IT security perception

In the study IT security perception has been evaluated so as to understand how employees perceive IT security according to their professions. Employees’ perceptions have been evaluated with what they know about IT security incidents

occurred in their companies. IT security incidents can be caused by both insiders and outsiders. Outsider related incidents were considered as network access attempt, access to company network, attack to Internet or telecommunication traffic, denial of service attack. Insider related incidents were abuse of Internet, abuse of company e-mail services, unauthorized access to system and data, violation of data protection regulations, abuse of confidential information, confidential data loss or leakage. Therefore, insiders and outsiders related security incidents which companies suffer from were asked to employees. Whether knowing insider and outsider related security incidents change based on employees' professions have been investigated.

Professions of employees were classified as IT related professions and non-IT related professions. Employees who are system administrator, software developer, project manager, IT consultant, IT personnel, web designer, database administrator, system analyst and business analyst were grouped as IT related professions, while employees working on departments not related to IT, such as finance and accounting, sales and marketing, human resources and after sales departments were classified as non-IT profession.

The most important result is that knowledge about insider related security incidents are not dependent on employees' professions, whereas knowledge about outsider related security issues depend on professions according to the 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. 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.

As it is seen in Figure 10, 38.21% of IT employees know outsider attacks whereas 13.21% of non-IT employees know those attacks according to the result of the study. Although proportion of non-IT employees who know outsider related security incidents in their companies is obviously low, they should have something in common with IT employees.

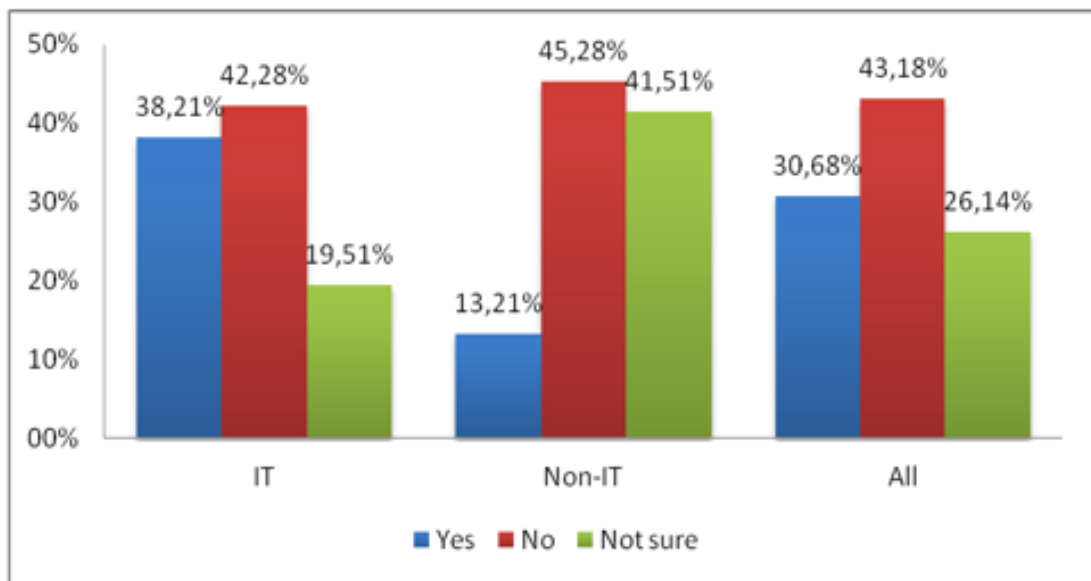


Figure 10. Answers of “were your company's systems attacked by an outsider in the last year?” classified by professions of employees

Source: (Tanriverdi & Metin, 2017)

After the finding about effect of professions, it is aimed to increase the understanding of how employees know security incidents. Employees are analyzed by how they are familiar with information security rather than just classifying them according to what their roles/jobs are in their companies. Employees’ familiarity with information security is considered as a capability to explain common points of 38.21% of IT employees and 13.21% of non-IT employees. Profession approach is targeted to be

enhanced with “information security familiarity” approach. In the sub-section, information security familiarity approach is explained.

3.2.2 Information security familiarity

The main approach of information security familiarity is to develop variables which measure experience and knowledge of employees. In order to achieve this aim, literature review is conducted as it is given in Chapter 2. As it is understood from reviewed literature; knowledge, experience and familiarity are related concepts according to usage in studies. It is seen from the literature that knowledge and experience are also used to predict security awareness. However, there is no work that test effects of both experience and knowledge directly on security awareness. In this study, knowledge and experience concepts are distinguished, reframed and approached differently. With this purpose, two concepts are defined in security context. What people know about threats and its countermeasures is evaluated as knowledge, while what kind of security incidents and precautions people ever have is evaluated as experience. Therefore, threat knowledge, protection knowledge, breach experience and protection indicator familiarity constitutes four areas of information security familiarity.

Even if literature studies measure familiarity in different context, most of them are directly asking research participants to evaluate themselves about how familiar with security they are. Thus, in this study measures are developed with the help of literature and security experts’ opinion to change this approach. Conducted work for expert opinion consulting is explained in Chapter 4. Description of variables are given as follows.

3.2.2.1 Knowledge: Threat knowledge and protection knowledge

Knowledge is usually approached having information about certain technology, platform and web sites which is out of security context in literature (Heartfield et al., 2016; Kelley & Bertenthal, 2016; Pattinson et al., 2012; Rhee et al., 2009; Yang et al., 2015). Studies reveal having information about those technologies and platforms are coming from direct or indirect experience like effects of what they learned from users (Nishioka et al., 2012; Yang et al., 2015). As it is understood that knowledge and experience can be mixed up in literature. With this aspect, it is essential to clarify knowledge concept.

On the other hand, the protection of systems from different security attacks is a constant challenge that many organizations face because of technological developments (Karyda, Kiountouzis, & Kokolakis, 2005) and advances in technology increase variety of threats and affect the way that users interact with technology (Kruger & Kearney, 2006). This makes users more vulnerable against to threats and requires applying protection methods regularly.

It shows critical role of employees' knowledge on protection methods against to threats as well as knowledge on threats itself. Most of studies measure either threats (Huang et al., 2007; Jeske & Schaik, 2017) or countermeasures (Furnell & Karweni, 1999; Lomo-David & Shannon, 2009; Luciano et al., 2010; Ng et al., 2009; Parson et al., 2014). That's why, in the knowledge side of information security familiarity, both threat knowledge and protection knowledge variables are considered to measure in this study.

3.2.2.1.1 Threat knowledge

Threat knowledge is measured with what employees know about various online threats in this study. Their knowledge on threats based on the classification of Jeske and Schaik on threats (2017) as the most traditional (virus, worm) and the most recent threats (social engineering, botnet, trojan, key logger and phishing) have been assessed. Some problems become frequently encountered problems because of increased technology usage by people in daily life and number of account they have online, such as identity theft (Jones, 2017). Accordingly, what kind of threats may lead identity theft is asked to measure threat knowledge. As Garg and Camp suggested in their study if respondents perceive threats accurately, they will find threats with the same risk (2012). Furthermore, employees' threat knowledge is measured by whether they are capable to distinguish almost the same threats. Virus and worm, for example, both are malicious software which replicate themselves. But, virus requires a human action and an infected host file, whereas worm do not require any of them (Cisco, n.d.). Besides technically similar threats, there are some concepts that are usually confused with each other, such as malware and spyware. Actually, malware is a general term that indicates all type of malicious software. Spyware is the one of malware which created with a specific purpose of collecting information from infected system (Panko & Panko, 2013).

3.2.2.1.2 Protection knowledge

Protection knowledge is evaluated with what employees know about protection methods of personal and private information, mobile devices, computers, Internet, network, social media and online services against mostly occurred threats, such as virus and malware infection, data breach and leakage. These threats are result in

serious damages like data loss, identity theft and even financial damages (The European Union Agency for Network and Information Security [ENISA], 2018). Online services which people mostly used in today's world, such as online banking, online shopping, e-mail services and services operated on mobile applications are included in the measure. Protection methods, including password management, access control, application management, network security management, protection from malware, are collection of information security best practices that what technology companies, finance institutions etc. suggest to their customers and users (Apple, n.d.1; Google, n.d.; Garanti, n.d.; Interbank Card Center [BKM], n.d.). These protection methods are also based on controls of ISO 27002 Information Technology Security Techniques Code of Practice for Information Security Controls that provides a reference for implementation of information security management system under the guidance of ISO27001 standard (International Organization for Standardization [ISO], 2013).

3.2.2.2 Experience: Breach experience and protection indicator familiarity

Experience is frequently evaluated in literature both as a predictor of security awareness (Haeussinger & Kranz, 2013; Johnston et al., 2010; Zhang & Li, 2015) and dimension of familiarity (Pattinson et al., 2012; Rhee et al., 2009). Mostly negative experience is considered in literature.

However, interaction with technology and systems do not have to be ended with negative consequences. While people are using operating systems, browsers, websites or platforms, they can encounter with notifications, alerts or indicators about security. Their main aim is to inform users about their current security situation.

Thus, experience of employees is considered with both consequences that makes them more familiar. Two of variables of experience are breach experience and protection indicator familiarity which are defined in following sub-section.

3.2.2.2.1 Breach experience

Breach experience is evaluated with what security breaches respondents have been experienced in this study. Breach types in the measure is gathered from existing literature and the trending security threats, such as unauthorized access to email accounts and social media accounts, having virus on PCs/laptops and mobile phones, data loss because of ransomware attack and financial fraud based on annual reports of ENISA (ENISA, 2018) and Kaspersky (Kaspersky, n.d.).

3.2.2.2.2 Protection indicator familiarity

If people are using specific platforms and technologies, they gain experience which makes them familiar with potential threats about platforms and technologies, and recognize threats timely compared to non-user of the platform. Being familiar with certain technology, platform, application or web site as it is named IT familiarity in several studies in literature (Heartfield et al., 2016; Kelley & Bertenthal, 2016; Pattinson et al., 2012; Rhee et al., 2009; Yang et al., 2015) is important factor.

However, it is obvious from these studies that they only measure how people's familiarity with the certain technology, platform or web site itself. In order to enhance this approach with information security context, interacting with technology, platform or web site through displayed notifications, alerts or indicators to users are evaluated as experience. Their common purposes are informing people

about possible consequences of their actions and attracting their notice about their security situation.

According to Zhang and Li (2015) frequency of having security warning messages are thought that how frequently a user encounters them, her/his security awareness are probably affected.

3.2.3 Security incident awareness

Awareness has been measured in many studies in different context (Bulgurcu et al., 2010; Haeussinger & Kranz, 2013; Hu & Dinev, 2007; Johnston et al., 2010; Ryan, 2007; Zhang & Li, 2015). In this study, awareness of security incidents which have occurred across Turkey or the world is considered. How well employees remember security incidents is associated with being aware of the incident, and causes and effects of incidents as well. Similar to Hu and Dinev's awareness approach (2007) which they have defined technology awareness as increased knowledge about technological issues in order to apply them, security incident awareness is considered as a state that enable employees to display appropriate behavior in order to prevent possibility of incidents.

Similarly, security incident awareness is measured in Tanriverdi and Metin's work as perception (2017) as it is previously mentioned it has been evaluated with occurred security incidents caused by insiders or outsiders. However, in this study security incident awareness variable is evaluated with whether employees know important security incidents instead of company specific issues in this study.

Selected security incidents have widespread media coverage between 2014 and 2018, and significant effect on individuals and/or companies in Turkey as well as all over the world. Problems which do not have a direct effect on people and/or

companies in Turkey have not been chosen even if it is claimed the biggest security breaches of recent history such as data breaches of Target stores in 2013 or Equifax data breach in 2017 according to security experts (Armerding, 2018) However, if target population of this study is considered as potential victims of similar breach, the security breach is asked. Questioned security incidents are carefully chosen in order to increase diversity of incidents based on technicality, popularity and locality.

Therefore, hypotheses given below is proposed in the first part of this study:

H1: Threat knowledge affects security incident awareness of employees positively

H2: Protection knowledge affects security incident awareness of employees positively

H3: Breach experience affects security incident awareness of employees positively

H4: Protection indicator familiarity affects security incident awareness of employees positively

3.3 Part 2: Effects of security incident awareness on security behavior

Companies' information security is directly affected by daily actions of their employees. In the second part of this study, how security incident awareness influences security behavior of employees is investigated. In several studies of literature, security awareness has been found as a significant predictor of security behavior which has been measured either actual behavior (AlKalbani et al., 2015) or intention to perform certain actions (Haeussinger & Kranz, 2013; Hu & Dinev, 2007; Johnston et al., 2010). Even if security behavior has not been evaluated with actual behavior which has been adapted in this study, several studies show that behavioral intention has a strong predictor of actual behavior (Limanyem & Hirt, 2003; Pahnla et al., 2007; Siponen et al. 2007; Siponen et al., 2010).

Thus, after having insight about factors having an effect on security incident awareness, whether employees' behavior in working environment are changing when

they are more aware of security incidents is aimed to be investigated in this study.

This part is considered as an enabler for putting inferences of this study into practice.

3.3.1 Information security behavior

Security behavior which have been studied many times in literature (AlKalbani et al., 2015; Limanyem & Hirt, 2003; Ng et al., 2009; Pahnla et al., 2007; Parson et al., 2014; Rhee et al., 2009; Siponen et al. 2007; Siponen et al., 2010). However, it is rarely measured with certain tasks performed by employees in working environment (Ng et al., 2009; Parson et al., 2014; Rhee et al., 2009) as it is intended to perform in this study.

Security behavior which reflects what employees are performing in working environment in certain tasks is measured in three focus areas; information handling, e-mail service usage and password management (Parson et al., 2014) in this study.

The hypothesis given below is proposed.

H5: Security incident awareness affects information security behavior of employees positively

CHAPTER 4

METHODOLOGY

In this chapter, data collection method of this study is described. Preparation of the questionnaire conducted within this study, questionnaire instruments, sampling design are also given in this chapter.

4.1 Data collection

Primary data is collected for this study via questionnaire in order to obtain structured quantitative data for testing of hypotheses. Questionnaire is prepared in online survey platform Lime Survey and it is published online.

Target population of this study is employees in Turkey who works with personal computer/laptop and uses Internet and email service for their daily work. Besides employees, prospective employees are also included in the population with the prerequisite of having a working experience in similar conditions. In this study, a specific sector is not chosen for target population. Employees from various departments contribute to our study because of the well-known fact that everybody is responsible for information security in any organization (Ross, 2011).

Accessibility of respondents is important criteria to use time effectively for data collection via questionnaire. For this reason, nonprobability sampling is designed for this study. Different nonprobability sampling techniques are used, these are convenience sampling, snowball sampling and self-selection sampling. At first, questionnaire sent to professional contacts of thesis author and thesis advisor via e-mail and requested to attend to the questionnaire. Although this type of sampling, namely convenience sampling, has a potential to make study more subjective, sectors

and departments of contacts are taken into consideration while choosing them.

Thanks to these contacts are from variety of sectors, such as banking, insurance, retirement, telecommunication, education, technology, public sector, consulting etc., subjectivity is kept minimum. These contacts were also asked to share the questionnaire with their colleagues, but at the end both attendance and distribution are based on voluntariness. This technique is known as snowball sampling that provides access to target population of interest. In addition to this, questionnaire was also distributed via LinkedIn. This is self-selection sampling that enables members of LinkedIn decide to attend to the questionnaire.

4.2 Research instruments

Conducted survey within this study has 34 close-ended questions in total including working information and company information questions, questions that measures variables of the research model, and demographic and technology usage profile questions (see in Appendix A). Turkish version of the questionnaire given in Appendix B is distributed to participants. Details of questions are explained in following sections.

4.2.1 Working information questions

There are three working information questions asked. Two of them are election questions in the survey for the participants about whether they are currently working first. This question is prepared in nominal scale and respondent gives a single answer that can be “yes” or “no”. Then, total working experience by year is asked. Working experience question is asked differently to respondents according to their answer for the working situation question in order to provide the consistency of answers of a

single respondent and have more accurate sample. If respondents are currently working, choices of second question are “less than one year”, “1 – 5 years”, “6 – 10 years”, “11 – 15 years”, “16 – 20 years”, “21 – 25 years”, “more than 25 years”. On the other hand, if respondents are not working currently, “I have no working experience” option is also appeared in answer part of second election question. Respondents who give the answer “I have no working experience” for second question are not suitable for sampling and are excluded from the dataset. 401 responses are collected in total, but 86 of them excluded from the sample because they do not have any working experience. So, study is conducted with the data of 315 respondents. Working area is third question that asks with “human resources”, “finance and accounting”, “marketing and sales”, “procurement”, “communication”, “law”, “operational functions”, “internal control and compliance”, “information security management”, “software development and business analysis”, “information systems network management”, “information systems infrastructure management”, “technical support and service desk management”, “information technology audit and consulting” and “other” choices. If respondents give “other” answer to company sector and working area questions, they are requested to specify them.

4.2.2 Company information questions

There are three questions that ask about company information of participants as multiple-choice question; company sector and company size. Company sector of respondents is asked in nominal scale including “automotive”, “consulting”, “construction”, “healthcare”, “education”, “technology”, “telecommunication”, “banking”, “insurance and retirement”, “energy and utilities”, “pharmaceutical”, “entertainment and media”, “tourism”, “retail and consumer products”, “industrial

products”, “public sector” and “other” options. Company size is asked in ordinal scale; “1 – 20”, “21 – 50”, “51 – 100”, “100 - 500“, “501 – 1000”, and “more than 1000”.

4.2.3 Variable questions

For measuring variables and testing hypotheses of research model 21 questions are asked. Variable, focus areas of variable, number of question and question types and scale of questions are summarized in Table 2, and explained in following sub-sections. Validity and reliability of these measures is important concern of this study. How to provide validity and reliability in this study is also explained accordingly.

Table 2. Summary of Variable Questions

Variable Name	Focus Areas	Number of Question and Question Types	Scale
Information Security Familiarity	Threat Knowledge	1 checkbox question, 2 multiple-choice questions	Nominal
Information Security Familiarity	Protection Knowledge	1 multiple-choice question	Multi-item (15 items), 5-point numerical
Information Security Familiarity	Breach Experience	6 multiple-choice questions	Nominal
Information Security Familiarity	Protection Indicator Familiarity	7 multiple-choice questions	Nominal
Security Incident Awareness	N/A	1 multiple-choice question	Multi-item (8 items), 5-point numerical
Information Security Behavior	E-mail service usage	1 multiple-choice question	Multi-item (4 items), 5-point Likert
Information Security Behavior	Password management	1 multiple-choice question	Multi-item (4 items), 5-point Likert
Information Security Behavior	Information handling	1 multiple-choice question	Multi-item (6 items), 5-point Likert

Validity and reliability of measures are ensured in this study. First of all, validity, mainly content validity, is considered as whether instruments actually measure

concepts desired to be measured. In this study content validity is aimed to be ensured with literature review study and expert opinion as Allen and Yen (1979) suggested in their research (as cited in Timmers & Glas, 2010, p. 55). Questions are created based on review of existent literature then expert opinion is consulted for security incident awareness, and information security familiarity's four focus areas, threat knowledge, protection knowledge, breach experience, protection indicator familiarity. Four experts who have an experience in IT governance and/or cyber security areas more than 10 years are consulted. Structure, scale and content of questions and items have been evaluated in order to ensure that content is complete and there is no ambiguity in questions. Questions are revised based on experts' opinion. In following paragraphs applied changes are explained in detail. After having final question set one expert who has been working IT governance area for four years, and four professionals who are working part-time in cyber security area have been consulted to assess questionnaire whether there is an unclear questions or answers. According to their comments, terminology used in questionnaire is updated.

Reliability of research model's three variables, protection knowledge, security incident awareness and information security behavior, is assessed with Cronbach's Alpha. According to reliability test results, variables have internal consistency. Reliability test results are given in Chapter 5.

4.2.3.1 Information security familiarity

Information security familiarity contains four focus areas; threat knowledge, protection knowledge, breach experience and protection indicator familiarity that have been measured by different questions.

4.2.3.1.1 Threat knowledge

Threat knowledge is one of information security familiarity variables whose measure is evaluated with security experts. Firstly, definitions of threats had been planned to evaluate threat knowledge of respondents as Jeske and Schaik have performed in their study (2017). However, creating different question structures instead of directly asking the definition has been considered with security experts with evaluating similar approach in literature (Garg & Camp, 2012). Besides format of question, content of question has been assessed with experts. The most frequent, traditional and sophisticated security threats have been determined to ask. At the end, nine different threats, virus, trojan, botnet, social engineering, worm, key logger, phishing, malware and spyware, have been assessed in totally three questions.

First of all, questions are asked in nominal scale then they converted to numerical values. Sum of the score of each question is calculated to measure respondent's threat knowledge. Questions and scales of this variable are given:

- In first question respondents' knowledge about identity theft is assessed. Seven threats, including virus, trojan, botnet, social engineering, worm, key logger, phishing, are given in options of checkbox question and asked to sign which threats are considered to result in identity theft. Four of them represent correct answers. For each correct answer (trojan, social engineering, key logger, phishing) three point is added to respondents, while only one point is added for each wrong answer. It is actually coming from adding one point for each correct answer and subtracting one point from total for each wrong answer. The reason of this scaling is having positive values while conducting analyses in SPSS. According to this scale respondents can have twenty-one points at most and seven points at least.

- Second and third questions evaluate whether respondent knows the differences between two similar threats. In second question virus and worm are questioned, whereas malware and spyware are asked in third one. Choices of these two questions are “yes”, “not sure”, “no”, then they are transformed to three, two and one point respectively. As a result, threat knowledge score ranges between nine and twenty-seven for a respondent.

4.2.3.1.2 Protection knowledge

Protection knowledge is measured as how effective the given protection methods are to ensure information and information systems’ security in a multi-item and 5-point numerical scale (1 is “not fully effective”, 5 is “fully effective”). In the protection knowledge measure, protection methods applied while using softcopy or hardcopy of information, connecting to a network or website, logging into a social media or e-mail account, making a transaction on Internet banking, using mobile device or computer have been involved. Not only online activities, but also offline activities and processes of people have been considered as focus areas of the measure.

While determine important protection methods, ISO27002 a code of practice for information security controls has been reviewed as well as existent literature. Security tips on technology and service usage given by technology giants like Google and Apple were also reviewed. In addition to this, security guides of Turkish banks and banking organizations, such as Interbank Card Center (BKM) and Garanti Bank were reviewed in order to create protection method questions about online and offline banking. Any item has not been asked in both protection knowledge and security behavior measures, even if the relationship between protection knowledge and security behavior would not been analyzed. 26 candidate questions were created

in aforementioned areas in total. However, some of questions have been eliminated with experts to keep questionnaire length reasonable. Which question is better to evaluate employees' protection knowledge is main approach while eliminating questions. Therefore, level of required knowledge for each protection method has been assessed by experts as low, medium and high in order to eliminate some questions.

On the other hand, some of the protection methods related to same tool and/or environment has been considered for elimination. For instance, antivirus software usage on mobile devices is asked, while updating virus definitions of antivirus software on computers is questioned. About password management, periodically changing passwords for social media and website accounts is asked, whereas complexity of password of wireless network connection is asked. Additionally, as an access management locking methods on mobile devices, and two-way authentication on e-mail services and social media user accounts, and logging out of user accounts while accessing with shared computers are considered. Application security on mobile is evaluated as having information about which data is shared with applications, and downloading application from official publisher, while computer application security is assessed with using only licensed version of software. Providing confidentiality of information is considered both in not sharing personal information via social media sites, not giving any banking information even verbally and keeping hardcopy documents closed and secure. Finally, unlike the purpose of all of the mentioned protection methods, backup is asked as a recovery method.

At the end of the evaluation, 15 protection methods given in Table 3 are determined for protection knowledge measure.

Table 3. Protection Knowledge Measure

Item Number	Item	Reference
Protection Knowledge_1	Periodically changing passwords of social media or website accounts	Adapted from (Interbank Card Center [BKM] Express, n.d.)
Protection Knowledge_2	Having a lock in mobile phones	Adapted from (Apple, n.d.1)
Protection Knowledge_3	Not doing any financial transaction via Internet when having public network connection	Adapted from (BKM, n.d.)
Protection Knowledge_4	Downloading mobile application only from official publisher	Adapted from (BKM Express, n.d.)
Protection Knowledge_5	Keeping virus definitions of antivirus protection software updated	Adapted from (BKM Express, n.d.)
Protection Knowledge_6	Not sharing banking information with bank personnel in any situation	Adapted from (BKM, n.d.)
Protection Knowledge_7	Carrying files and documents including important information with a cover	Self-developed
Protection Knowledge_8	Not sharing personal information on social media, even if having only close friends and relatives as a connection on social media	Self-developed
Protection Knowledge_9	Not downloading free software via web sites which has normally licensing fee	Adapted from (BKM Express, n.d.)
Protection Knowledge_10	Having complicated password of wireless network connection at home	Self-developed
Protection Knowledge_11	Having antivirus software in mobile phones	Adapted from (BKM Express, n.d.)
Protection Knowledge_12	Using two-way authentication in e-mail service and social media accounts	Adapted from (Google, n.d.)
Protection Knowledge_13	Checking which services the application can access before downloading the application	Adapted from (Apple, n.d.1)
Protection Knowledge_14	Safely logging out from e-mail service or social media sites in commonly used PC or laptops	Self-developed
Protection Knowledge_15	Backing up important folders and documents	Adapted from Rhee et al. (2009)

4.2.3.1.3 Breach experience

Breach experience is one of information security familiarity variables that whether employees have ever experienced any breaches which are the most frequently encountered security incidents, such as virus infection on mobile devices, data loss because of ransomware, financial fraud, unauthorized access to email and social media accounts. First of all, questions have been created to be more specific in terms of attack vector and consequences of the attack. For example, questions with item number BreachExperience_1 and BreachExperience_2 (see Table 4) have been prepared so as to specify the result of phishing attack, instead of only asking whether

they have phishing attack as Rhee et al. have evaluated in their study (2009). Moreover, according to ENISA's Threat Landscape Report ransomware attacks increasingly occurred in 2017 (2018). It has been mentioned in the report that ransomware supposedly had over five-billion-dollar global damage in 2017. Therefore, ransomware (item number; BreachExperience_5) has been asked in breach experience measure. During the recent years, in Turkey many people have fallen a victim of social engineering conducting via telephone or social media that causes financial loss (Elçiboğa, 2018). Thus, this breach experience is included in measure. In addition to this, because %23 of occurred security incidents were virus/malware/Trojan in business according to Kaspersky (n.d.), it is also involved in this measure. After creating these questions, they have been assessed with security experts. Expert has been suggested to add virus infection on mobile devices (item number; BreachExperience_3). However, which operating system respondents have in their mobile devices have also been asked in questionnaire, as it is previously mentioned in this chapter, because of the fact that mobile devices with iOS operating systems do not require antivirus protection (Apple, n.d.2). After consulting expert opinion, six questions given in Table 4 are included. Questions are developed in nominal scale. Choices of questions are "yes", "not sure", "no", then they have been converted to numerical values as three, two and one points respectively. Sum of the given answers is calculated to measure breach experience score of respondents. Thus, breach experience score ranges between six and eighteen.

4.2.3.1.4 Protection indicator familiarity

Protection indicator familiarity is the last information security familiarity variable measured in this study. Which notification, warning or indicator related security

protection have been experienced by employees is evaluated. Aim of this variable is to measure employees' security experiences except experiences which have negative consequences.

Table 4. Breach Experience Measure

Question Number	Question Statement	Reference
Breach Experience_1	Have you ever experienced unauthorized access to email accounts?	Adapted from Rhee et al. (2009)
Breach Experience_2	Have you ever experienced unauthorized access to social media accounts or user account of any website?	Adapted from Rhee et al. (2009)
Breach Experience_3	Have you ever experienced virus infection on their PCs/laptops?	Adapted from Rhee et al. (2009)
Breach Experience_4	Have you ever experienced virus infection on mobile devices?	Self-developed
Breach Experience_5	Have you ever experienced data loss because of ransomware attack?	Adapted from (ENISA, 2018; Kaspersky, n.d.)
Breach Experience_6	Have you ever experienced financial fraud as a result of drawn bank account, credit card information out of you?	Adapted from (ENISA, 2018; Kaspersky, n.d.)

Having experience in some tools and technologies are associated with familiarity with those tools and technologies (Heartfield et al., 2016; Kelley & Bertenthal, 2016; Pattinson et al., 2012; Rhee et al., 2009; Yang et al., 2015). With using same logic information security technology usage can be evaluated as positive security experience. This approach is criticized with security experts. Because protective information security technology is maintained centrally in the most of companies, employees do not have to use protection solutions like antivirus software. On the other hand, certain usage of information and information systems is defined as security behavior within this study. Thus, it is decided that usage of various IT tools and platforms are chosen to be asked instead of information security technologies.

As it is investigated in Kelley and Bertenthal's study (2016), signs which indicate security protection level are considered as protection indicator familiarity variable. Protection indicators which users have come across while using Internet

and online services, such as e-mail, online shopping and online banking are included in the measure. However, indicators asked in this study vary from platform to platform. That's why, any notification, warning or indicator is not described in question as it is made in Kelley and Bertenthal's study.

Totally seven questions given in Table 5 are developed and evaluated with experts. Questions are asked in nominal scale and answers of questions are "yes", "not sure", "no", then they are transformed to three, two and one point respectively. Thus, protection indicator familiarity score ranges between seven and twenty-one for a respondent.

Table 5. Protection Indicator Familiarity Questions

Question Number	Question	Reference
ProtectionIndicator Familiarity_1	Have you ever have a notification about security scanning of downloaded e-mail attachments?	Self-developed
ProtectionIndicator Familiarity_2	Have you ever have a notification about security scanning of file downloaded from web site?	Self-developed
ProtectionIndicator Familiarity_3	Have you ever seen https connection in Internet banking and online shopping web site?	Self-developed
ProtectionIndicator Familiarity_4	Have you ever have a certification error warning in Internet browser?	Self-developed
ProtectionIndicator Familiarity_5	Have you ever have a network connection warning about having shared wireless?	Self-developed
ProtectionIndicator Familiarity_6	Have you ever seen an indicator related to powerfulness of password while creating in email service or social media sites?	Self-developed
ProtectionIndicator Familiarity_7	Have you ever have an e-mail notification from e-mail services or social media sites for logging in from another device?	Self-developed

4.2.3.2 Security incident awareness

Security incident awareness is assessed with how well employees remember eight different security incidents in a multi-item question. The question has eight items and all of the items are self-developed. Questioned security incidents are summarized from articles or reports of journals and newspapers. Scale of the question is 5-point numerical scale (1 is "I do not remember at all" and 5 is "I remember very well").

Scale is evaluated with security experts in terms of scope of the security incident, level of interest, effects of the incident to validate whether it actually reflects security incident awareness of participants. At the beginning 10 questions have been chosen among important security incidents which had widespread media coverage in Turkey between 2013 and 2018, and significant effect on individuals and/or companies all over the world and/or Turkey. But, two of them have been extracted after interviews with experts. One of the excluded security incident is Russian interference in the 2016 USA elections (Harding, 2016). It is determined that security incidents should be chosen among problems which somehow affects Turkish people. Other one is data breach of Yahoo which 3 billion user accounts compromised in 2013 (Armerding, 2018). In order to reduce the effect of time on memorability, this one has been excluded.

Final eight security incidents given in Table 6 are determined based on point of interest they have got to be aware of. For example, some incidents' (item number; SecurityIncidentAwareness_1, SecurityIncidentAwareness_2, SecurityIncidentAwareness_6, and SecurityIncidentAwareness_8) technical side are dominant. Therefore, people should have even a little technical knowledge. On the other hand, some of security incidents (item number; SecurityIncidentAwareness_3, SecurityIncidentAwareness_4) are more related to Turkish people because of the victim of these incidents is Turkish people. Also, victim of some incidents (item number; SecurityIncidentAwareness_5 and SecurityIncidentAwareness_7) are popular people or companies all around the world.

Table 6. Security Incident Awareness Measure

Item Number	Item	Reference
SecurityIncident Awareness_1	In recent years, ransomware has threatened users. This ransomware has encrypted all files in systems after opening the attachment or links within a received e-mail which pretends as if send by GSM operators or Internet service providers.	Adapted from (Onat, 2016)
SecurityIncident Awareness_2	Wannacry ransomware has spreaded to 200.000 systems within 3 days in almost 150 countries because of a vulnerability of Microsoft Systems. Especially operations of hospitals, telecommunication companies and automotive sector were highly effected.	Adapted from (CyberMag, n.d.)
SecurityIncident Awareness_3	In 2016, identity information of approximately 50 million Turkish Republic citizens have been leaked. Database which includes identity information has been provided in the Internet by hackers. Leaked database has included 46 million 611 thousand 709 citizens' TR identity number, mother and father name, date of birth and residence address.	Adapted from (50 Milyon Vatandaşın, 2016)
SecurityIncident Awareness_4	Power outage which was occurred across Turkey at the beginning of 2017 has become a controversial issue because of spoken cyber-attack suspicion.	Adapted from (2 Yıl Önce Türkiye, 2017)
SecurityIncident Awareness_5	In August 2017, HBO producer of the most popular television series of recent years Game of Thrones has announced that their 1.5 TB data has been leaked which includes the seventh season of Game of Thrones.	Adapted from (NTV, 2017)
SecurityIncident Awareness_6	In December 2016, one of the most leading banks in Turkey has announced that their SWIFT international money transfer system has been cyber attacked.	Adapted from (Sezer & Altayli, 2016)
SecurityIncident Awareness_7	Between 2014 and 2017 some Hollywood celebrities' private photographs on iCloud have been hacked and shared publicly on the Internet.	Adapted from (ShiftDelete.Net, 2017)
SecurityIncident Awareness_8	WPA2 protocol which is the most secure and widespread wireless connection encryption method has been hacked.	Adapted from (Beyhan, 2017)

4.2.3.3 Information security behavior

Information security behavior is evaluated with agreement of whether they apply given behaviors in three focus areas adapted from Parson et al.'s work; e-mail service usage, password management and information handling (2014). Parson et al. (2014) have evaluated, such sub-areas as unauthorized software installation, dubious website access, and inappropriate internet use under focus areas. These controls are usually monitored centrally and automatized in large size companies. However, sample is not controlled based on respondents' company sizes in this study. Thus, it is decided that those areas are not involved in the measure.

Question is prepared in multi-item and 5-point agreement Likert scale (“strongly disagree”, “disagree”, “neither agree nor disagree”, “agree”, “strongly agree”). There are totally 14 items under three focus areas including both adapted and self-developed items. Measure is given in Table 7.

Table 7. Information Security Behavior Measure

Focus Area	Item Number	Item	Reference
Email service usage	EmailUsage_1	Before reading an email, I first check if the subject and the sender make sense.	Adapted from Ng et al. (2009)
	EmailUsage_2	Before opening an email attachment, I first check if the filename of the attachment makes sense.	Adapted from Ng et al. (2009)
	EmailUsage_3	I exercise caution when I receive an email attachment as it may contain a virus.	Adapted from Ng et al. (2009)
	EmailUsage_4	I do not open email attachments if the content of the email looks suspicious.	Adapted from Ng et al. (2009)
Password management	Password Management_1	Before leaving in front of my computer/laptop, I first lock my system	Adapted from Rhee et al., (2009)
	Password Management_2	I use different passwords for different software, programs and systems	Adapted from Rhee et al., (2009)
	Password Management_3	To remember my password, I write on a notebook or something on my desk	Adapted from Rhee et al., (2009)
	Password Management_4	I do not share my personal account information with my colleagues	Self-developed
Information handling	Information Handling_1	I do not leave sensitive material unsecure	Adapted from Rhee et al., (2009)
	Information Handling_2	I delete information on USB devices after transferring it	Self-developed
	Information Handling_3	I pay attention whether data is encrypted in the data transfer platform which has been shared with me by third parties	Self-developed
	Information Handling_4	I do not share my computer with anybody (family member, colleague or customer)	Adapted from Rhee et al., (2009)
	Information Handling_5	I destroy sensitive documents securely	Adapted from Rhee et al., (2009)
	Information Handling_6	I do not help people who I do not know to enter my company’s building	Self-developed

4.2.4 Demographic profile questions

After hypotheses testing questions, three demographic questions which are; gender, age and education are positioned in the questionnaire. All of them are prepared as multiple-choice question. Gender is asked in nominal scale. Age is asked in ordinal scale whose choices are “under 20”, “20 – 25”, “26 – 30”, “31 – 35”, “36 – 40”, “41 – 45”, “above 45”. Education is prepared in nominal scale including “High-school”, “associate degree”, “bachelor degree”, “master degree”, “doctorate degree” choices.

4.2.5 Technology usage questions

Finally, four questions about technology usage;

- Number of years in having a social media account
- Number of years in having a mobile phone
- Operating system of mobile phone
- Internet browsers frequently used in mobile phone and PC/laptop

are asked to respondents.

Technology usage questions are also prepared to determine technology affinity of the sample. Participants are questioned that how many years they are having a social media account and a mobile phone. These questions are prepared in ordinal scale including “I don’t have any”, “less than one year”, “1 – 3 years”, “4 – 6 years”, “7 – 10 years” and “more than 10 years” options. Operating system of mobile phone of participants are asked in nominal scale including “Android”, “iOS”, “Windows”, “other”. Finally, the most frequently used Internet browsers in mobile phone and PC/laptop are asked to participants in nominal scale. Choices are “Google Chrome”, “Firefox”, “Internet Explorer”, “Safari” and “other”.

CHAPTER 5

ANALYSES AND FINDINGS

In this chapter, analyses of responses are presented. Descriptive findings, reliability analysis of scales, multiple regression and linear regression analyses between variables are given. Data set collected from online survey platform are analyzed with using IBM SPSS Statistics (SPSS). Data set is first cleaned with Microsoft Excel to eliminate unsuitable data for sampling then it is imported to SPSS. Data is labeled and coded in SPSS to prepare it for analyses.

5.1 Descriptive findings

Descriptive statistics of demographics, company information, working information and technology usage are given by frequency and percentage. Statistics of three variables of the research model are also given in this chapter.

5.1.1 Demographic profile of respondents

Gender, age and education of respondents are analyzed. According to results given in Table 8, 56.5% of respondents are male, when 43.5% of them are female. Almost the half of respondents (46.7%) are between 26 and 30 years old. Most of them (69.2%) has bachelor degree.

Table 8. Demographic Profile of Respondents

	Variables	Frequency	Percent
Gender	Male	178	56.5
	Female	137	43.5
Age	Below 20	1	0.3
	20-25	73	23.2
	26-30	147	46.7
	31-35	42	13.3
	35-40	24	7.6
	41-45	17	5.4
	Above 45	11	3.5
Education	Doctorate	9	2.9
	Master	69	21.9
	Bachelor	218	69.2
	Associate	10	3.2
	High School	9	2.9
Total		315	100

5.1.2 Company information of respondents

As it is seen in Table 9 that respondents are coming from big size companies mostly. Companies of 55.9% of respondents have more than 1000 employee. When it comes to company sector, they are coming from various sectors, however consulting, technology, banking, telecommunication and education are the most dominant sectors respectively.

Table 9. Company Information of Respondents

Variables		Frequency	Percentage
Company Size	1-20	38	12.1
	21-50	21	6.7
	51-100	11	3.5
	101-500	38	12.1
	501-1000	31	9.8
	Above 1000	176	55.9
Company Sector	Consulting	91	28.9
	Technology	54	17.1
	Banking	31	9.8
	Telecommunication	26	8.3
	Education	23	7.3
	Public Sector	14	4.4
	Insurance and Retirement	10	3.2
	Industrial Products	8	2.5
	Retail and Consumer Products	8	2.5
	Entertainment and Media	7	2.2
	Automotive	7	2.2
	Healthcare	7	2.2
	Construction	6	1.9
	Energy and Utilities	4	1.3
	Pharmaceutical	4	1.3
	Tourism	4	1.3
Other	11	3.3	
Total		315	100

5.1.3 Working information of respondents

After electing respondents who are not working currently and have no experience, rest of respondents' working information are analyzed. According to results given in Table 10 92.7% of respondents are currently working. Rest of them have at least 1 year and less experience. 61.9% of respondents are considered as beginners who have less than 5-year experience. This distribution provides a sample less affected by corporate culture. It can be accepted that their behaviors do not become habit. 26.7% of them have between 5 and 15-year experience, while 11.4% of them have more

than 15-year experience. When they have classified with respect to their professions as IT and non-IT, it is seen that there is almost equally distributed sample according to profession.

Table 10. Working Information of Respondents

Variables		Frequency	Percent
Working Status	Working	292	92.7
	Not working	23	7.3
Working Experience	Below 1 year	39	12.4
	1-5 years	156	49.5
	6-10 years	56	17.8
	11-15 years	28	8.9
	16-20 years	20	6.3
	21-25 years	10	3.2
	Above 25 years	6	1.9
Profession	IT Related	162	51.4
	Non-IT Related	145	46.0
	Other	8	2.5
Total		315	100

5.1.4 Technology usage of respondents

According to Table 11 technology usage of respondents are adequate for this study in terms of technology usage duration. They can be accepted as longtime technology users. Results show that 54% of respondents have been using smartphone for 7 years and above, while 46% of them 6 years and below. Additionally, 83.5% of respondents have been using social media for 7 years and above, while 16.5% of them 6 years and below.

Based on their operating system and Internet browser usage certain OS and Internet browsers dominate others. Dominant operating system is iOS, while Google Chrome and Safari are the most frequently used Internet browsers. 60.3% of respondents are using phone with iOS. 45.7% of respondents are using Google

Chrome in their smartphones, and 43.8% of them are using Safari. On the other hand, 83.2% of them prefer Google Chrome for PC/laptop.

Table 11. Technology Usage of Respondents

Variables		Frequency	Percent
Smartphone Usage	Below 1 year	1	0.3
	1-3 years	14	4.4
	4-6 years	130	41.3
	7-10 years	116	36.8
	Above 10 years	54	17.1
Social Media Usage	Below 1 year	2	0.6
	1-3 years	6	1.9
	4-6 years	44	14.0
	7-10 years	154	48.9
	Above 10 years	92	29.2
	Non-user	17	5.4
Operating System of Smartphone	Android	119	37.8
	iOS	190	60.3
	Windows	2	0.6
	Other	4	1.3
The most used Internet Browser in Smartphone	Firefox	11	3.5
	Google Chrome	144	45.7
	Internet Explorer	9	2.9
	Safari	138	43.8
	Other	13	4.1
The most used Internet Browser in PC/Laptop	Firefox	22	7.0
	Google Chrome	262	83.2
	Internet Explorer	12	3.8
	Safari	8	2.5
	Other	11	3.5
Total		315	100

5.1.5 Descriptive statistics of variables of research model

Descriptive statistics of three variable of research model are given in this section.

These are threat knowledge, breach experience and protection indicator familiarity.

Mean values of these questions are given Table 12. Mean value of threat knowledge

is 19.45 out of 27. Breach experience has mean of 8.58 out of 18 that it is less than

average value. Mean of protection indicator familiarity of 19.09 is also quite high.

Besides mean and standard deviation values, frequencies of questions of these three

variables are given in following paragraphs.

Table 12. Descriptive Statistics of Threat Knowledge, Breach Experience and Protection Indicator Familiarity Variables

Variable	Mean	Std. Dev.
Threat Knowledge	19.45	2.32
Breach Experience	8.58	2.13
Protection Indicator Familiarity	19.09	2.50

5.1.5.1 Threat knowledge

As it is explained in Chapter 4 threat knowledge includes three questions that first question is checkbox question. Four options (trojan, social engineering, key logger, phishing) are correct answer of the question, while three of them (virus, worm, botnet) are incorrect. At least 57.5% of respondents mentioned that threat given in options is the correct answer of question except botnet choice. That's why only 6.7% of respondents give correct answer to virus, 7.9% of them to worm and 7.9% of them to botnet. The most "uncertain" answer (56.2% of respondents) is given to botnet.

According to result of second and third questions, 32.1% of respondents claimed that they know the difference between virus and worm, while 26.3% of them know the difference between malware and spyware. These ratios are actually very low. All results of threat knowledge variable are given in Appendix C.

5.1.5.2 Breach experience

More than 80% of respondents claimed that they have not been experienced e-mail account or social media account theft, ransomware attack, financial fraud or virus infection on mobile phone. On the other hand, 64.1% of respondents mentioned they have haven computer virus.

It is interesting point that 7.3% of respondents claimed that they are not sure whether their computers have infected before whereas this rate is 14.3% in mobile virus infection cases. Additionally, the highest “not sure” answer is given to mobile virus infection. 60.3% of respondents are using iOS mobile phones, this can be the reason why “not sure” answer is given at most among other breaches. Moreover, respondents probably are not familiar with the effect of virus infection on mobile phone and they do not know how to understand if they have infected. Financial fraud question which has the most tangible consequence, financial loss, has been answered only six times (1.9%) as “not sure”. That’s why, it can be a good approach to measure breach experience with the consequences of breaches and how to detect if they experience any incident. Detailed results are given in Appendix C.

5.1.5.3 Protection indicator familiarity

75% of respondents have positively answered protection indicator familiarity questions. The highest response is given to question which asks indicator related to powerfulness of password, 93.3% of respondents mentioned they have ever seen this indicator. The second highest response, 91.7% of respondents, is given to e-mail notification coming from e-mail services or social media sites to inform users about that their account has been accessed from another device. Rest of results are given in Appendix C.

5.2 Reliability and descriptive statistics of multi-item scale questions

Reliability of three multi-item scale questions, protection knowledge, security incident awareness, and information security behavior, of the survey are checked by Cronbach’s Alpha. Acceptable level of Cronbach’s Alpha is 0.7 (Hair, Anderson,

Tatham, & Black, 1995). According to results given in Table 13 three variables have internal consistency.

Table 13. Reliability/Internal Consistency of Survey Items

Survey Items	Number of Items	Cronbach's Alpha
Protection knowledge	15	0.889
Security incident awareness	8	0.813
Security behavior	14	0.822

Details of the reliability tests and descriptive statistics of variables are provided in following sub-sections.

5.2.1 Reliability analysis for protection knowledge

Protection knowledge scale which includes 15 items is tested to see whether items are consistent with each other. According to the test results Cronbach's Alpha is 0.889. Detailed reliability test results are given in Appendix D. Because the value is higher than 0.7, protection knowledge scale is reliable with 15 items. It means that arithmetic mean of all items are calculated to measure protection knowledge score.

5.2.2 Descriptive statistics of protection knowledge

After testing reliability of protection knowledge variable, descriptive statistics are evaluated. Mean values of each items are given in Table 14. Items are measured on 5-point numerical scale that 1.00 corresponds to "the least important" and 5.00 "the most important". Mean values show that respondents' protection knowledge is higher than average value.

Table 14. Mean Values of Protection Knowledge

Protection Knowledge		n	Mean	Std. Deviation
Protection Knowledge_1	Periodically changing passwords of social media or website accounts	315	3.86	1.155
Protection Knowledge_2	Having a lock in mobile phones	315	4.30	0.908
Protection Knowledge_3	Not doing any financial transaction via Internet when having public network connection	315	4.26	0.949
Protection Knowledge_4	Downloading mobile application only from official publisher	315	4.13	0.995
Protection Knowledge_5	Keeping virus definitions of antivirus protection software updated	315	4.20	0.987
Protection Knowledge_6	Not sharing banking information with bank personnel in any situation	315	4.58	0.799
Protection Knowledge_7	Carrying files and documents including important information with a cover	315	4.42	0.799
Protection Knowledge_8	Not sharing personal information on social media, even if having only close friends and relatives as a connection on social media	315	4.16	0.993
Protection Knowledge_9	Not downloading free software via web sites which has normally licensing fee	315	3.83	1.147
Protection Knowledge_10	Having complicated password of wireless network connection at home	315	4.22	0.967
Protection Knowledge_11	Having antivirus software in mobile phones	315	3.56	1.213
Protection Knowledge_12	Using two-way authentication in e-mail service and social media accounts	315	4.21	0.951
Protection Knowledge_13	Checking which services the application can access before downloading the application	315	4.18	0.993
Protection Knowledge_14	Safely logging out from e-mail service or social media sites in commonly used PC or laptops	315	4.50	0.724
Protection Knowledge_15	Backing up important folders and documents	315	4.41	0.875
Protection Knowledge_AVG	Average Protection Knowledge	315	4.1873	0.60767

5.2.3 Reliability analysis for security incident awareness

Cronbach's Alpha value of security incident awareness is 0.813 which is greater than 0.7. Result shows that there is an internal consistency among eight items as it is seen in Appendix D. Mean value of security incident awareness is calculated with eight items.

5.2.4 Descriptive statistics of security incident awareness

Mean values of each items are given in Table 15. Scale of security incident awareness measure is 5-point numerical scale (1.00 is "I do not remember at all" and 5.00 is "I remember very well"). The highest rates are given respectively to Turkish Republic identity data leakage with the mean of 4.24, iCloud hacking of Hollywood celebrities with 4.08, widespread power outage in Turkey with 3.97, Game of Thrones HBO Hack with 3.95. All of these security incidents are about either local issues or related to popular culture. On the other hand, security incidents which have more technical side have lowest mean values. These are WPA2 vulnerability and KRACK attack with the mean of 2.69, Wannacry attack with 3.37, SWIFT hack in a Turkish Bank with 3.45, and ransomware attacks with 3.59.

Table 15. Mean Values of Security Incident Awareness

Security Incident Awareness Items		n	Mean	Std. Deviation
SecurityIncident Awareness_1	Ransomware attacks	315	3.59	1.468
SecurityIncident Awareness_2	Wannacry attack	315	3.37	1.597
SecurityIncident Awareness_3	Turkish Republic identity data leakage	315	4.24	1.207
SecurityIncident Awareness_4	Widespread power outage in Turkey	315	3.97	1.312
SecurityIncident Awareness_5	Game of Thrones HBO Hack	315	3.95	1.531
SecurityIncident Awareness_6	SWIFT hack in a Turkish Bank	315	3.45	1.506
SecurityIncident Awareness_7	iCloud hacking of Hollywood celebrities	315	4.08	1.325
SecurityIncident Awareness_8	WPA2 vulnerability and KRACK attack	315	2.69	1.594
SecurityIncident Awareness_AVG	Average Security Incident Awareness	315	3.6667	0.95302

Note: Given items represent short version of security incidents awareness items

5.2.5 Reliability analysis for information security behavior

Information security behavior scale includes 14 items. One of items is recoded because it is questioned reversely. Reliability of information security behavior scale is checked. Cronbach's s Alpha is 0.822 according to the results given in Appendix D. The value shows that items of the scale are consistent with each other. So, mean of 14 items are calculated to measure security behavior.

5.2.6 Descriptive statistics of information security behavior

Descriptive statistics is evaluated and given in Table 16. Question is asked in 5-point agreement Likert scale (1: “strongly disagree”, 2: “disagree”, 3: “neither agree nor disagree”, 4: “agree”, 5: “strongly agree”). Average of security behavior is 4.20 which is quite high.

5.3 Hypotheses tests

Hypotheses (H1, H2, H3 and H4) are tested with multiple regression analysis in order to figure out the effects of information security familiarity on security incident awareness. Effects of security incident awareness on security behavior (H5) is also tested with linear regression analysis.

5.3.1 Multiple regression analysis for testing part 1

Protection knowledge, threat knowledge, breach experience and protection indicator familiarity are considered that they have an effect on security incident awareness. In order to evaluate the effect of these four variables on security incident awareness, multiple regression analysis is conducted.

Multiple regression analysis is one of multivariate data analysis methods which is usually used for prediction problems with assessing the relationship between dependent variable and independent variables (Hair et al., 1995). In multiple regression analysis, there is a single dependent (criterion) variable and several independent (predictor) variables.

Table 16. Mean Values of Information Security Behavior

Security Behavior		n	Mean	Std. Deviation
EmailUsage_1	Before reading an email, I first check if the subject and the sender make sense	315	4.40	0.909
EmailUsage_2	Before opening an email attachment, I first check if the filename of the attachment makes sense	315	4.28	0.916
EmailUsage_3	I exercise caution when I receive an email attachment as it may contain a virus	315	4.26	1.013
EmailUsage_4	I do not open email attachments if the content of the email looks suspicious	315	4.63	0.742
Password Management_1	Before leaving in front of my computer/laptop, I first lock my system	315	4.40	1.046
Password Management_2	I use different passwords for different software, programs and systems	315	3.77	1.247
Password Management_3_recode	To remember my password, I write on a notebook or something on my desk	315	4.3841	1.19516
Password Management_4	I do not share my personal account information with my colleagues	315	4.36	1.135
Information Handling_1	I do not leave sensitive material unsecure	315	4.51	0.886
Information Handling_2	I delete information on USB devices after transferring it	315	3.87	1.140
Information Handling_3	I pay attention whether data is encrypted in the data transfer platform which has been shared with me by third parties	315	3.45	1.208
Information Handling_4	I do not share my computer with anybody (family member, colleague or customer)	315	4.08	1.092
Information Handling_5	I destroy sensitive documents securely	315	4.03	1.147
Information Handling_6	I do not help people who I do not know to enter my company's building	315	4.40	0.964
Security Behavior_AVG	Average Security Behavior	315	4.2014	0.57954

At the end of the analysis a regression equation is estimated and shows the effect of predictors on criterion variable. Equation given below shows predictors (X_1, X_2, \dots, X_n) and a criterion variable (Y). In the equation, (β_0) corresponds to the intercept (constant) term, (β_1) is the regression coefficient and e is error term (residual) of the equation. Error term represents the difference between the observed value and estimated value caused by non-estimated predictor variables.

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \dots + \beta_n X_n + e$$

Multiple regression analysis makes certain assumptions in order to make sure that this analysis is suitable to apply to the data intended to be analyzed (Cohen, Cohen, West, & Aiken, 2003; Laerd Statistics, 2015a). If any assumption is violated, it creates some concerns about correctness and appropriateness of the regression model. Specification of the model becomes problematic (Cohen et al., 2003). When any violation of assumption is diagnosed, remedial actions should be taken properly and the assumption should be re-tested. Other analyses can be required when remediation does not work. For this reason, assumptions are controlled before interpreting of the regression analysis results and equation.

In following sub-sections assumptions test and multiple regression test results are given respectively.

5.3.1.1 Assumption test for part 1

Assumptions of multiple regression analysis are autocorrelation (serial correlation), linearity, homoscedasticity of residuals, not having multicollinearity, normality of residuals (Cohen et al., 2003; Laerd Statistics, 2015a). These assumptions are explained and test results of assumptions for multiple regression analysis of part 1 are given in following paragraphs.

Autocorrelation is subject of time-series studies (Cohen et al., 2013; Pindyck & Rubinfeld, 1991). Residuals can be correlated with observations which can be systematically change over time. That's why, there is no need to test autocorrelation for this study.

Linearity is the first assumption which should be controlled. Because multiple regression analysis is an extension of simple linear regression, linearity must be met in multiple regression analysis (Cohen et al., 2003; Laerd Statistics, 2015a).

Linearity is controlled in two aspects. First one is establishing the form of the relationship between each independent variable and dependent variable. In order to control the form of the relationship between them, scatterplot of dependent variable against each independent variable is created separately. According to scatterplots there is a linear relationship between each three independent variables (protection knowledge, threat knowledge, breach experience) and dependent variable (security incident awareness) whereas relationship between protection indicator familiarity and security incident awareness does not present linearity apparently (see in Appendix E). However, form of the relationship is accepted linear and protection indicator familiarity is not excluded from regression analysis.

Second aspect for linearity assumption is checking whether there is a linear relationship between dependent variable and independent variables collectively. To control this scatterplot of residuals against predicted variable of the regression model is plotted. Multiple regression analysis is conducted with four independent variables and dependent variable to calculate unstandardized predicted value and studentized residual values. Scatterplot is constructed and established with using these values. Lowess (loess) fit line which is drawn by iterative weighted least square is added to scatterplot so as to see if there is a systematic deviation of residuals from 0-line

(IBM Knowledge Center, n.d.1). As it is seen in Figure 11 loess line follows 0-line.

It means that there is no systematic relationship between residuals and predicted values. Therefore, linearity assumption is met for the data set of this study.

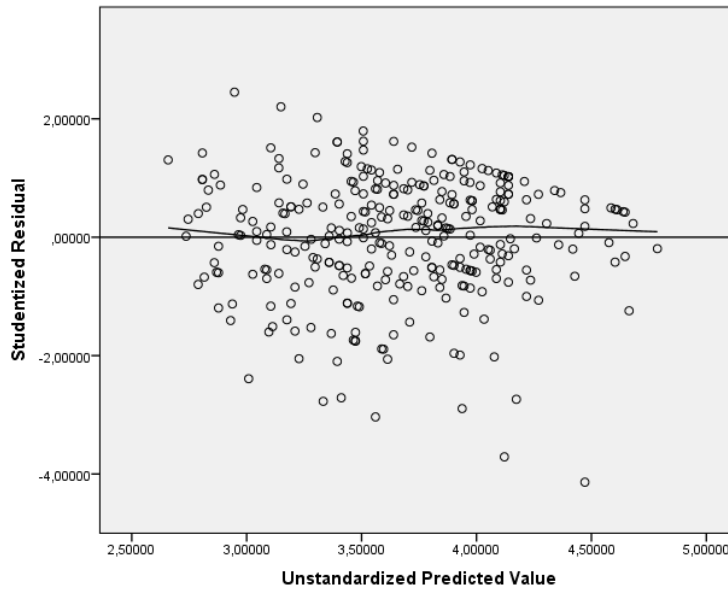


Figure 11. Scatterplot of studentized residual against unstandardized predicted value

Homoscedasticity is other assumption to be checked. If variance of the residuals is constant, there is homoscedasticity of residuals (Cohen et al., 2003; Laerd Statistics, 2015a). In case of heteroscedasticity, efficiency and reliability of regression model reduces and remedial actions are required (Gujarati, 1988). In order to detect heteroscedasticity in the data there are different methods suggested, such as graphical method, Park test, Breusch-Pagan test, Spearman's rank correlation test etc. (Gujarati, 1988). In graphical methods, homoscedasticity is controlled by scatterplot of estimated residuals against predicted values which is previously constructed for checking of linearity. Figure 11 does not show an apparent pattern between residuals and predicted values. Spearman's rank correlation test is also applied so as to make sure that there is no heteroscedasticity in the data. In this test, whether there is a

correlation between absolute value of unstandardized residuals and independent variables are controlled by Spearman's rank correlation coefficient (Gujarati, 1988). As it is seen in Table 17 there is no significant correlation coefficient value between absolute values of residuals and independent variables at 0.05 significance level or even 0.1 significance level. Therefore, homoscedasticity assumption is met for the data set.

Table 17. Spearman's Rank Correlation Test Results

		abs RES_1	Protection Knowledge _AVG	Breach Experience	Security Protection Indicator	Threat Knowledge
abs RES_1	Correlation Coefficient	1.000	-0.006	-0.004	-0.101	-0.088
	Sig. (2-tailed)	0.0	0.917	0.946	0.074	0.117
	N	315	315	315	315	315

Multicollinearity is another focus of multiple regression analysis that occurs, if there are high relations between independent variables in the regression model (Cohen et al., 2003; Laerd Statistics, 2015a). Multicollinearity leads complications in the interpretation of the regression model. Multiple regression analysis assumes that independent variables are not correlated with each other. Degree of multicollinearity is evaluated by assessing tolerance and variance inflation factor (VIF) values. If tolerance value is less than 0.1, which makes VIF higher than 10, multicollinearity problem occurs in data set. As it is seen in Table 18, all tolerance values are higher than 0.1. Thus, there is no multicollinearity between variables. This assumption is also met.

Table 18. Tolerance and VIF Values of Variables

Variables	Tolerance	VIF
ThreatKnowledge	0.962	1.040
ProtectionKnowledge_AVG	0.962	1.040
BreachExperience	0.967	1.034
ProtectionIndicatorFamiliarity	0.883	1.132

Normality of residuals is the final assumption of multiple regression analysis to be tested in this study. Residuals of regression line is assumed that it is normally distributed for any independent variable value (Cohen et al., 2003). Violation of normality assumption does not make serious problems for regression results especially in significance test and confidence intervals based on the sample size. It may point problems on specification of regression model. There are two graphical examination methods for checking the normality of residuals; histogram and p-p plot (Laerd Statistic, 2015a). Firstly, histogram of residuals is plotted. Figure 12 shows approximately normal distribution with approximately zero mean value and standard deviation of 0.997. Additionally, in Figure 13 it can be seen that there are some deviations from regression line. It can be claimed that residuals of the regression model are approximately normally distributed because of robustness of regression analysis against to deviations from normal distribution (Laerd Statistics, 2015a). As a result of assumption tests any problem is not detected related to assumptions.

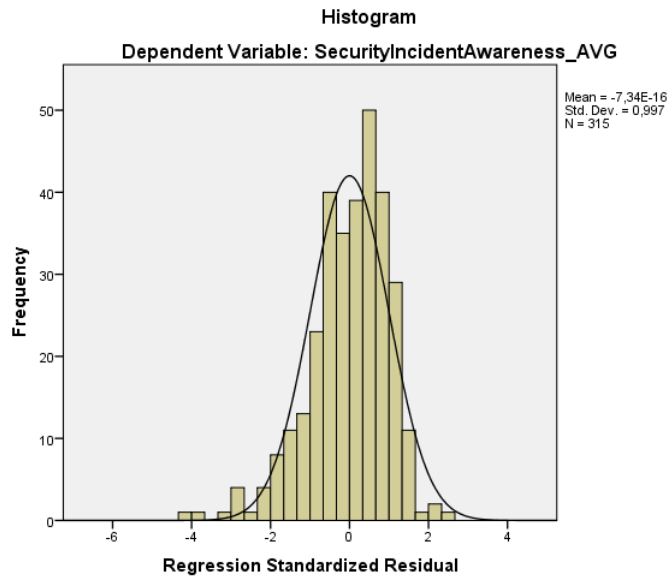


Figure 12. Distribution of residuals

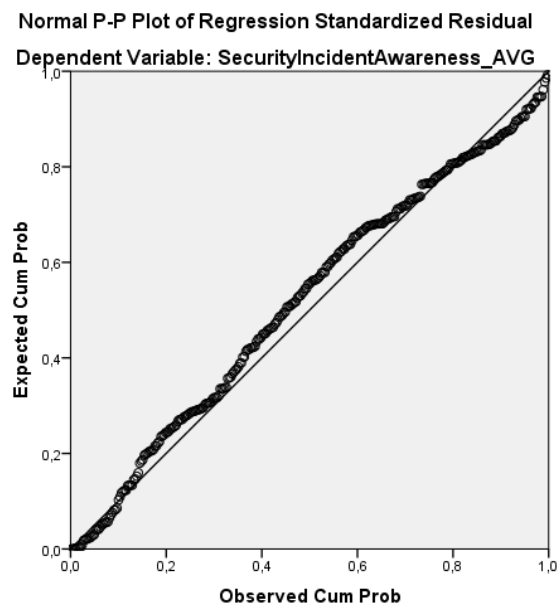


Figure 13. P-P plot of residuals

5.3.1.2 Multiple regression test results for part 1

According to assumption test results, sample is adequate for multiple regression analysis. Therefore, regression model is estimated and fitness of regression model is evaluated in this section.

In order to eliminate insignificant variables from regression model, stepwise regression is applied. In stepwise estimation predictor variables are sequentially selected for the regression model according to the contribution of the variable to the regression model (Hair et al., 1995). In this method, it usually begins with simple linear regression model constituted by the most powerful predictor and criterion variables. The most powerful predictor variable is the most highly correlated variable with dependent variable. And stepwise estimation procedure continues with searching next predictor variable which can significantly explain the largest portion of remaining error from simple linear regression, in order to put it to the model. For this purpose, partial correlation coefficients are examined within the procedure. After adding another variable regression equation is re-built and F value is recalculated. F value is examined to see whether the model is still significant. At the end of the process the most powerful model to predict criterion variable is computed. To apply this method linear regression functionality of SPSS is used in stepwise method with default settings. Probability of F is used as a stepping method criteria and entry value is determined by 0.05 while removal value is 0.1 in default settings of stepwise regression method.

Stepwise regression analysis has run two steps and reached final result. In the first step threat knowledge is entered. According to the first model's statistics R^2 value is 0.192 with an adjusted R^2 of 0.189 (see in Appendix F). In the second step protection knowledge are added to the regression model. R^2 value increased to 0.219 and adjusted R^2 0.214. R^2 value shows how good is the model, in other words it is "goodness of fit" measure (Cohen et al., 2003). It also shows proportion of the variance of dependent variable. However, R^2 overestimates proportion of variance, so adjusted (corrected or shrunken) R^2 is also calculated to have more accurate

insight about the model. According to the results, threat knowledge and protection knowledge can explain 21.4% of the usage of security incident awareness which is above of acceptable level of 10% according to Falk and Miller (1992) (as cited in Ng et al., 2009, p. 822).

The results of second model of multiple regression indicates that two of variables, threat knowledge and protection knowledge, significantly affects security incident awareness, $F(2, 312) = 43.732$, $p < 0.0005$, $\text{adj. } R^2 = 0.214$.

As it is given in Table 19 regression coefficient of protection knowledge is 0.263 whereas threat knowledge's 0.166. It shows that protection knowledge affects security incident awareness better than threat knowledge.

Table 19. Summary of Multiple Regression Analysis

Variable	Unstandardized Coefficient	Standardized Coefficient (B)	t-value (p-level)
Constant	-0.671		-1.408 (0.160)
Threat knowledge	0.166	0.405	7.944 (0.000)
Protection knowledge	0.263	0.168	3.290 (0.001)
F (p-value) = 43.732 (0.000)			
R^2 (R^2 adjusted) = 0.219 (0.214)			

According to the stepwise regression results breach experience and protection indicator familiarity which are excluded from regression model do not significantly affect security incident awareness (Table 20)

Table 20. Excluded Variables of Regression Model

Variable	Beta in	t-value (p-level)
Breach experience	-0.073	-1.441 (0.151)
Protection indicator familiarity	0.091	1.724 (0.086)

According to regression equation given below one unit increase in protection knowledge leads security incident awareness increased to 0.263 unit, while threat knowledge makes 0.166 unit increase.

Security Incident Awareness

$$= -0.671 + 0.263 * \text{Protection Knowledge} + 0.166 * \text{Threat Knowledge}$$

Hypotheses can be interpreted according to the multiple regression analysis results. Two of hypotheses are accepted whereas other two are rejected.

One of accepted hypotheses is H1 (Threat knowledge affects security incident awareness of employees positively). Results of multiple regression reveal that threat knowledge has significant effect on security incident awareness at 0.0005 significance level.

Hypotheses H2 (Protection knowledge affects security incident awareness of employees positively) is also accepted. According to test results protection knowledge significantly influences security incident awareness at 0.005 significance level.

On the other hand, Hypotheses H3 (Breach experience affects security incident awareness of employees positively) is rejected because related variable, breach experience, is not a significant factor that has an effect on security incident awareness at even 0.1 significance level.

Hypotheses H4 (protection indicator familiarity affects security incident awareness of employees positively) is also rejected. Multiple regression results show that protection indicator familiarity does not influence security incident awareness at 0.05 significance level.

5.3.2 Linear regression analysis for testing part 2

Simple linear regression analysis is intended to conduct in second part of the research model which includes security incident awareness as an independent variable and information security behavior as a dependent variable. It is expected that there is a positive linear relationship between security incident awareness and security behavior. In order to assess the form of the relationship between independent variable and dependent variable, scatterplot is created and loess fit line is added to the scatterplot. It is observed that there is a curvilinear relationship between security incident awareness and security behavior given in Figure 14.

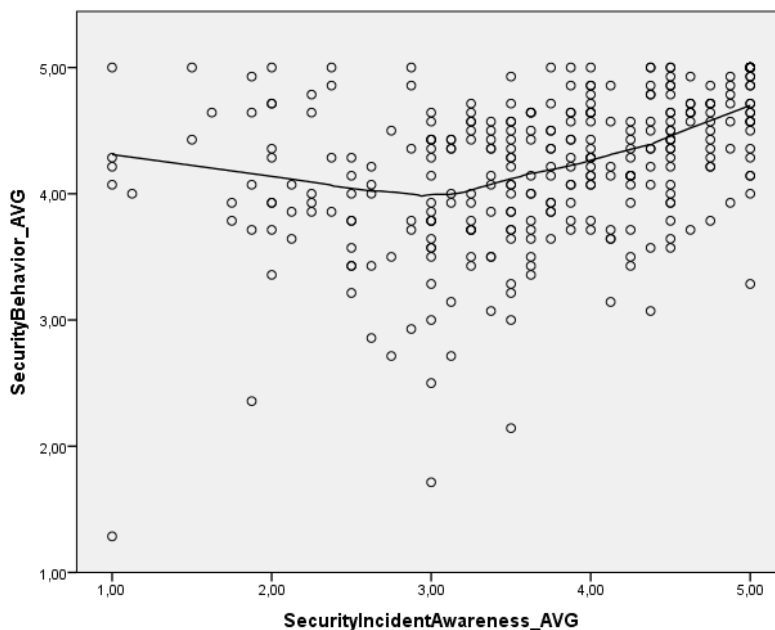


Figure 14. Scatterplot of security behavior against security incident awareness

This curvilinear relationship between these variables can be explained with polynomial (curvilinear) regression. However, the form of the relationship between security incident awareness and security behavior is criticized before modelling.

As it is seen in Figure 14, security behavior of respondents is slightly decreasing when security incident awareness increases at the security incident

awareness level between 1.00 and 3.00 over 5.00. Then security behavior starts to increase at the value 3.00 by security incident awareness. Between 3.00 and 5.00 positive linear relationship occurs between variables as it is predicted. It is observed that there are 60 respondents (19.05% of total respondents) who have security incident awareness value less than 3.00. 60 respondents' demographics, working information, company information and technology usage descriptive statistics and security behavior descriptive statistics is assessed in following paragraphs.

Demographics, working information, company information and technology usage are evaluated to analyze whether there is an apparent characteristic occurred. When 60 respondents' demographics are analyzed (see in Appendix G), it is understood that there is no apparent difference in distributions of education level and age. Only difference occurs in gender. Male respondents are dominant in whole sample whereas female respondents are dominant in 60 of sample. Company information (company sector, company size) of 60 respondents are not different from whole population (see in Appendix G). Dominant sectors (insurance, telecommunication, technology, banking etc.) are same in two of the samples. When company size is separated as below and above 500 people, distribution is appeared almost same. Technology usage of two samples is also compared (see in Appendix G). There is no apparent difference between two sample in smartphone usage (by years), social media usage (by years), operating system of smartphone. Internet browser usage in both smartphone and PC/laptop are slightly different. According to working information frequencies of working experience of 60 respondents are almost same with original sample (see in Appendix G). However, it is observed that distribution of the profession of respondents are different in two samples. In original sample distribution of IT and non-IT related professions are almost equal (non-IT

related professions by 46%, IT by 51.5%, others by 2.5%), while non-IT related professions are dominant among 60 respondents with 60% (IT related professions by 36.7%, others by 3.3%). Profession's effect on security incident awareness has been investigated in prior study as it is discussed in Chapter 3. Thus, it can be seen that non-IT related professions may negatively affect security incident awareness based on the findings of prior study. Although there is a difference in terms of distribution of profession, other descriptive statistics does not reveal apparent variance.

60 respondents' answers to security behavior questions show that minimum 1 and maximum 5 have been given to security behavior questions by them (see in Appendix G). Their answers do not seem certain characteristics in any way except average score of security behavior 4.01 of 60 respondents which is less than overall sample's average score 4.20 (see in Appendix G).

People who have less than 3.00 point at security incident awareness are not considered as a healthy sample to evaluate security behavior because of given answers to security behavior. Additionally, 60 respondents' demographics, working information, company information and technology usage is almost same as overall sample except professions whose effect on security incident awareness has been studied previously. That's why, 60 respondents, who are small proportion of all respondents (19.05%), can be neglected to assess the relationship between security incident awareness and security behavior. Besides, additional analyses are conducted in order to assess how the model is affected when 60 respondents are excluded from the sample (see the sub-section 5.3.3.1).

After excluding 60 respondents, linear regression analysis is conducted. In following sections assumption test results and regression test results are given accordingly.

5.3.2.1 Assumption test and remedial actions for part 2

Assumption of linear regression is linearity, homoscedasticity and normality of residuals. Linearity condition is met (Figure 15). However, it is detected that there is heteroscedasticity in data. So, weighted least square (WLS) regression is applied as a remedial action (Cohen et al., 2003). There is decreasing linear relationship between independent variable and residuals as it is seen in Figure 16. Therefore, weight is calculated with the inverse of the square of the predicted value (Cohen et al., 2003). The predicted value is computed at the linear regression which is secondly conducted with security incident awareness as an independent variable and the absolute of the residual of the first conducted linear regression as a dependent variable (H. Michael Crowson, 2015).

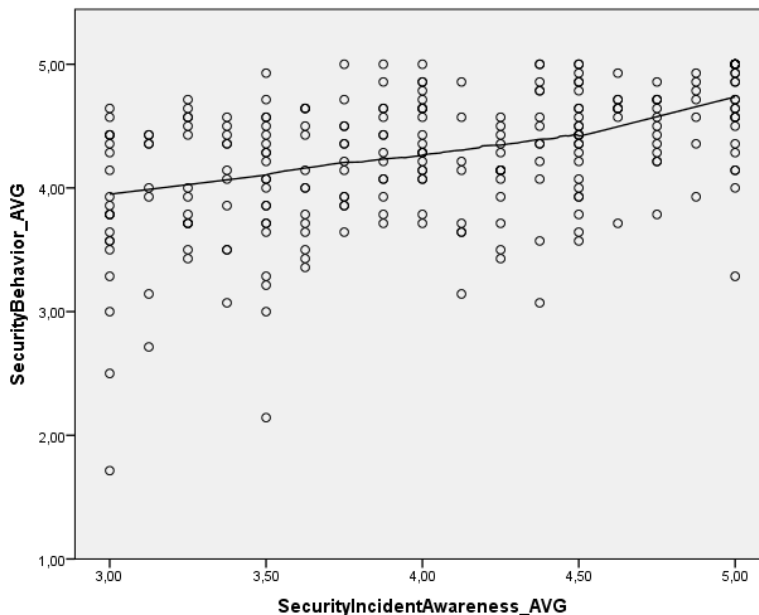


Figure 15. Scatterplot of security behavior against security incident awareness

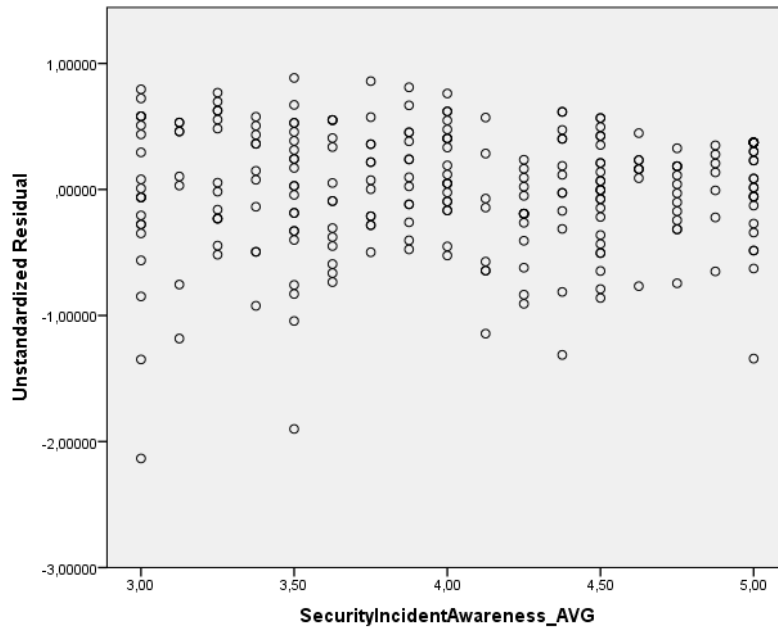


Figure 16. Scatterplot of residual of the model against security incident awareness

After calculating weight, weighted least square regression with the calculated weight value is conducted between security incident awareness and security behavior (Cohen et al., 2003; H. Michael Crowson, 2015).

Residual and predicted value of WLS regression are calculated to draw scatterplot for homoscedasticity check. So, following equations are computed to calculate them; weighted predicted value = unstandardized predicted value * $\sqrt{\text{weight}}$, weighted residual value = unstandardized residual value * $\sqrt{\text{weight}}$ (IBM Knowledge Center, n.d.2). According to scatterplot of weighted residual value against weighted predicted value given in Figure 17, homoscedasticity is met after conducting WLS regression.

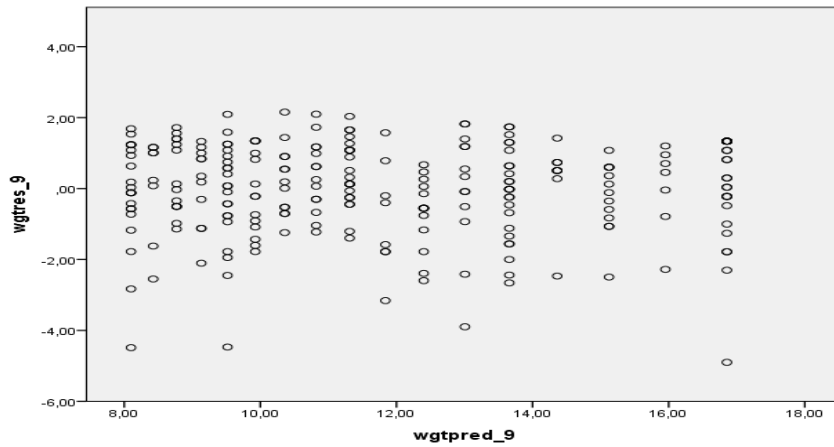


Figure 17. Scatterplot of weighted residual value against weighted predicted value

As it is seen in Figure 18 and Figure 19 weighted residuals of WLS regression is almost normally distributed with 0 mean value and 1.274 standard deviation.

According to (Minitab, 2014) sample sizes 15 and grater are not sensitive to non-normal distribution of residuals (as cited in Laerd Statistics, 2015b).

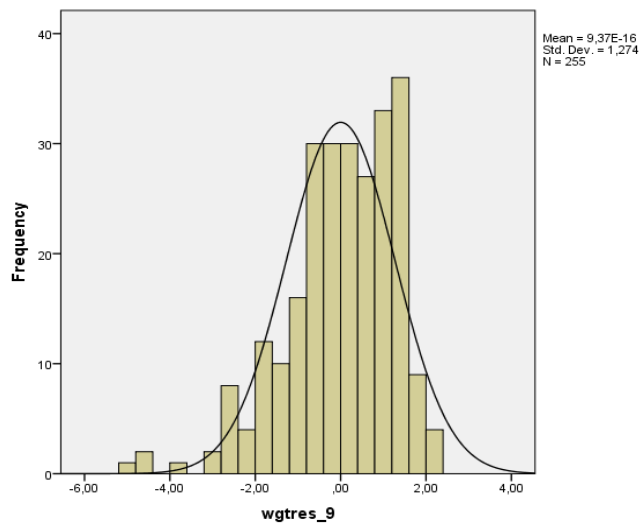


Figure 18. Distribution of weighted residuals of WLS regression

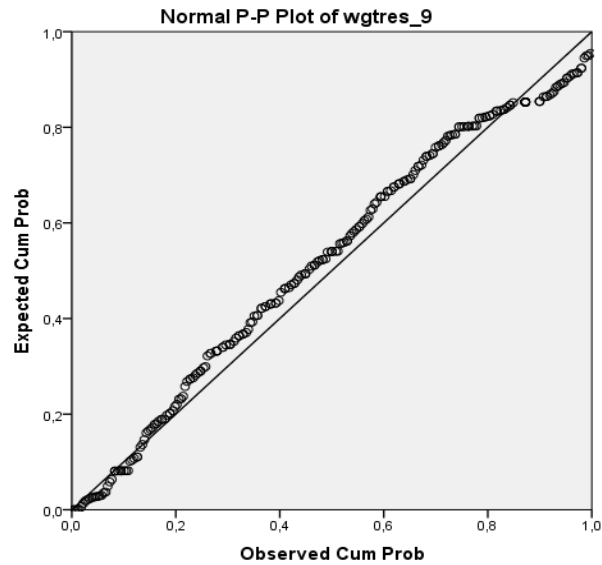


Figure 19. P-P plot of weighted residuals of WLS regression

5.3.2.2 Weighted least square regression test results of part 2

As a result, security incident awareness significantly affects security behavior, $F(1, 253) = 73.230$, $p < 0.0005$. 22.4% of the variation in security behavior with adjusted R^2 0.221 is accounted by security incident awareness (see Appendix H). According to test results, regression equation is:

$$\text{Security Behavior} = 2.657 + 0.395 * \text{Security Incident Awareness}$$

It means that one unit change on security incident awareness leads 0.395 unit change on security behavior.

5.3.3 Additional test results and important findings

In order to expand the insight about the results of conducted analyses, additional tests, multiple regression test and independent sample t-test are performed.

5.3.3.1 Multiple regression test of part 1 after excluding 60 responses

To see the effect of excluding responses who have security incident awareness value less than 3.00 on Part 1, multiple regression analysis is conducted stepwise again with the sample from which excluded 60 respondents. Stepwise regression built three models that third model shows that R^2 and adjusted R^2 value increased to 0.239 and 0.230 respectively (see in Appendix I). Furthermore, three of variables which are threat knowledge, protection knowledge and breach experience significantly affect security incident awareness, $F(3, 251) = 26.308$, $p < 0.0005$, $\text{adj. } R^2 = 0.230$. As it is given in Table 21 regression coefficient of threat knowledge is 0.110 whereas protection knowledge's 0.175. Protection knowledge again explains security incident awareness better than other variables. Moreover, breach experience is also found as a significant variable at 0.05 significance level. One unit change in breach experience value leads -0.039 unit change on security incident awareness.

Table 21. Summary of Multiple Regression Analysis

Variable	Unstandardized Coefficient	Standardized Coefficient (B)	t-value (p-level)
Constant	0.517		1.252 (0.212)
Protection knowledge	0.175	0.158	2.782 (0.006)
Threat knowledge	0.110	0.394	7.010 (0.000)
Breach Experience	-0.039	-0.131	-2.329 (0.021)
F (p-value) = 26.308 (0.000)			
R^2 (R^2 adjusted) = 0.239 (0.230)			

5.3.3.2 Difference between professions with respect to threat knowledge and protection knowledge

Relationship between IT/non-IT profession and information security familiarity has not been included in the research model, because the aim of this study is enhancing profession point of view a step further. However, in order to make more accurate

suggestions based on the findings of this research, whether there is a difference between two profession groups (IT and non-IT) of employees with respect to threat knowledge and protection knowledge, whose effects on security incident awareness are proven in this research, is analyzed. Independent-samples t-test is used to analyze whether there is a significant difference between IT and non-IT profession groups.

In the sample, there are 162 respondents with IT profession and 145 respondents with non-IT profession. 8 of respondents which cannot be classified as IT or non-IT are not involved in independent samples t-tests. Independent samples t-test run in order to evaluate differences in threat knowledge score between IT professionals and non-IT professionals first. According to results of this test, there is significant difference between IT professionals and non-IT professionals, $M = 1.583$, 95% CI[1.085, 2.081], $t(296.368) = 6.252$, $p = 0.000$. Threat knowledge of IT professionals ($M = 20.20$, $SD = 2.144$) is higher than non-IT professionals ($M = 18.62$, $SD = 2.276$) (see Appendix J).

According to the result of independent samples t-test which is conducted to test whether there is a difference between IT professionals and non-IT professionals with respect to protection knowledge, protection knowledge of IT professionals ($M = 4.240$, $SD = 0.552$) is higher than non-IT professionals ($M = 4.113$, $SD = 0.663$). However, there is no significant difference between two group of employees with the statistics $M = 0.127$, 95% CI[-0.01069, 0.26524], $t(281.416) = 1.816$, $p = 0.07$. Detailed test results of independent samples t-test are given in Appendix J.

5.3.3.3 Difference between genders with respect to security incident awareness and security behavior

Among 60 respondents whose security incident awareness level is less than 3.00 female employees are dominant. Thus, whether gender makes a difference in security incident awareness is tested with using independent-samples t-test. According to the test results there is a significant difference between female and male employees, $M = -0.452$, 95% CI[-0.656, -0.247], $t(306.961) = -4.352$, $p = 0.000$. security incident awareness of male employees ($M = 3.86$, $SD = 0.975$) is higher than female employees ($M = 3.41$, $SD = 0.862$) (see Appendix K)

Whether there is a difference between female and male employees with respect to security behavior is analyzed. It is found that there is no significant difference between female and male employees with the statistics $M = -0.068$, 95% CI[-0.19481, 0.5971], $t(308.343) = -1.044$, $p = 0.297$ (see Appendix K).

CHAPTER 6

DISCUSSION AND CONCLUSION

In this chapter results of hypotheses tests and important findings are discussed and concluded, and suggestion related to findings are given. Future studies are also mentioned.

6.1 Discussion

People have become more involved the information oriented world and more integrated with information security systems. Within current technology ecosystem digital business model becomes more important. According to results of information security survey conducted globally by PricewaterhouseCoopers (PwC), 63 percentage of respondents claimed that their companies run their information technology (IT) function in the cloud. The 36 percentage of respondents are running their operation function in the cloud, while the percentage of customer service is 36, market and sales is 34 and finance function is 32 in the cloud (2016). With the effect of digitalization, information security becomes more and more important. According to 59 percentage of respondents of global information security survey, digitalization leads companies to increase spending on security (PwC, 2016). Additionally, people become more involved the information oriented world and more integrated with information security systems. Thus, skills of employees should be adapted to the new conditions. That's why, this study is important to create a knowledge in terms of information security behavior and awareness.

The aim of this study was investigating effect of information security familiarity factor on security incident awareness and at the same time analyzing how

security incident awareness affects information security behavior. With this purpose online survey has been conducted to collect data to analyze five hypotheses suggested in this study. Totally 315 employees who work at companies located in Turkey have been used to analyze hypotheses. The study includes two parts. At the first part, effect of information security familiarity on security incident awareness has been investigated. In the second part, how employees' security incident awareness level affects their security behavior has been tested.

6.1.1 Information security familiarity measure

Information security familiarity was considered as an extension of IT/non-IT profession approach which has been researched in prior study (Tanriverdi & Metin, 2017b). In the study, effect of employees' profession on their knowledge/awareness about security incidents caused by insiders (abuse of Internet, company e-mail services and information, unauthorized access to system and data, violation of data protection regulations, confidential data loss or leakage) and outsiders (network access attempt, access to company network, attack to Internet or telecommunication traffic, denial of service attack) suffered in their companies have been searched. The result of study has shown that knowledge about insider related security incidents are not dependent on employees' professions, whereas knowledge about outsider related security issues depend on professions. To investigate information security familiarity as the common point of IT people and non-IT people who know insider/outsider security incidents of their companies was triggered by the result of Tanriverdi and Metin's study.

Thus, information security familiarity variable was measured in four areas based on literature review and information security and IT governance experts'

opinions. Those were threat knowledge, protection knowledge, breach experience, and protection indicator familiarity. Four hypotheses were suggested in the first part of this research. According to hypotheses test results conducted by multiple regression analysis, effect of threat knowledge and protection knowledge on security incident awareness has been proven. However, breach experience and protection indicator familiarity have been found that they do not significantly affect security incident awareness.

6.1.2 Significant information security familiarity factors

Knowledge factors, threat knowledge and protection knowledge, have been found that they have an effect on security incident awareness. As several studies have measured knowledge concept as a familiarity (Furnell & Karweni, 1999; Huang et al., 2007; Jeske & Schaik, 2017; Lomo-David & Shannon, 2009; Luciano et al., 2010; Ng et al., 2009; Parson et al., 2014), knowledge which have been measured in the context of information security in this study as threat knowledge and protection knowledge can represent information security familiarity.

Protection knowledge which shows knowledge about effective countermeasures against to threats significantly influence security awareness according to results. It was measured broadly with effective protection methods applied while using softcopy or hardcopy of information, connecting to a network or website, logging into a social media or e-mail account, making a transaction on Internet banking, using mobile device or computer.

Threat knowledge which was measured with the knowledge about the most traditional, frequent and sophisticated threats have been found as a significant factor on security incident awareness. Having knowledge on threats affects security

incident awareness positively according to test results. Recognizing the difference between similar concepts and attacks was a dimension of threat knowledge measure. With the measure not only knowing concepts but also recognizing nuances between them has been found an influencing factor on security incident awareness.

Although, protection knowledge is 1.6 times better than threat knowledge to explain security incident awareness according to multiple regression equation, knowledge about threats and differences of threats significantly influence security awareness.

6.1.3 Effects of employee profession on information security familiarity

In order to make more accurate suggestions based on the findings of this research, whether there is a difference between two profession groups (IT and non-IT) of employees with respect to threat knowledge and protection knowledge was analyzed.

According to the results there is a significant difference between IT professionals and non-IT professionals with respect to threat knowledge. However, there is no significant difference between two groups of employees according to protection knowledge. Similar to finding of prior study, threat knowledge which requires more technical point of view is higher in IT professionals than non-IT professionals.

6.1.4 Security incident awareness, benchmarking and security behavior

In the second part of the study, whether employees' behavior in working environment are changing when they are aware of security incidents was another focus of this study. Hypothesis suggests that employees' security incident awareness positively affects their information security behavior in working environment.

However, according to scatterplot of security behavior against to security incident awareness, there has been a curvilinear relationship between security incident awareness and security behavior. Security behavior is decreasing when security incident awareness score ranges between 1.00 and 3.00. Then security behavior starts to increase at the value 3.00 by security incident awareness. Between 3.00 and 5.00 positive linear relationship occurs between variables as it is predicted. This unexpected situation makes a think of which level of employees' security incident awareness is trustable. There are 60 respondents (19.05% of total respondents) who have security incident awareness value less than 3.00. These respondents mostly have non-IT related professions (60% of them). Thus, it can be seen that non-IT related professions may negatively affect security incident awareness based on the findings of prior study (Tanriverdi & Metin, 2017b). Also, 51.7% of them are female and according to the additional test results security incident awareness of female employees are worse than male employees.

This study is limited to explain security behavior with security incident awareness. And it is possible to investigate factors create decreasing relationship between security incident awareness and security behavior at the range of one to three. But, it is very important finding that security incident awareness can be evaluated as a significant benchmark with threshold value three out of five under the setting of this study in order to assess security behavior of employees.

Additional analysis has been conducted to test Part 1 with 255 respondents. Breach experience has become a significant factor of security incident awareness. Breach experience measure is related to security incidents in employees' own lives, while security incident awareness is about incidents occurred around the world

and/or Turkey. This result can show employees' general approach to security incidents.

Moreover, according to analysis conducted after excluding 60 respondents, security incident awareness significantly affects security behavior. One unit change on security incident awareness leads 0.395 unit positive change on security behavior.

6.1.5 Finding about insignificant information security familiarity factors

Breach experience which was measured with whether employees have ever experienced any breaches which are the most frequently encountered security incidents, such as virus infection on computers and mobile devices, data loss because of ransomware, financial fraud, unauthorized access to email and social media accounts is not a significant factor of security incident awareness. When we look at the statistics of breach experience, more than 80% of respondents claimed that they have not been experienced e-mail account or social media account theft, ransomware attack, financial fraud or virus infection on mobile phone. This situation may cause insignificance of breach experience on security incident awareness in the model.

Besides, after excluding respondents who are not aware of security incidents, breach experience has become a significant factor of security incident awareness at 0.05 significance level. One unit change in breach experience leads -0.039 unit change on security incident awareness. This result shows contrast to literature studies which have found positive effect of negative experiences on security awareness (Haeussinger & Kranz, 2013; Johnston et al., 2010). However, it can be caused by magnitude of experience which has been emphasize on Chen and Zahedi's study (2016). If any attack does not result in any loss, such as data, file or financial loss or even time, it may not influence to person. Moreover, result can also be explained in

other factors which have not been tested within this study like self-efficacy. Rhee et al. (2009) shows in their study that having negative experience decreases self-efficacy of victims. They have found that when a person has experienced any security breaches, their belief about themselves to deal with security incidents, like virus infected folders/files, deleting malware, consulting help for security problems, using protective applications and setting different security levels in browsers and even understanding information security related concepts are decreased. They have also claimed that negative security experiences lead to stress and anxiety which have been evaluated another type of loss in Chen and Zahedi's study (2016).

Protection indicator familiarity was also found that it does not have an effect on security incident awareness. It has been measured with security experiences of employees except experiences which have negative consequences, such as faced notification, warning and indicator related to security. 75% of respondents have positively answered to protection indicator familiarity questions. This situation may affect the results. Additionally, other studies have shown that using same platforms, web sites and technologies becomes habit in time. Having the same security warnings, notifications and indicators on the screen may become a usual case for respondents like using a same platform as other studies found (Heartfield et al., 2016; Kelley & Bertenthal, 2016; Pattinson et al., 2012; Rhee et al., 2009; Yang et al., 2015)

6.2 Conclusion

To sum up, in order to improve security behavior of employees in working environment, they should more aware of security incidents. Security incident awareness scale, which is one of original practices in this area as a measure, can be

used for benchmarking to evaluate the security awareness level of employees, and how much effort they require to reach a certain level of security awareness and accordingly security behavior. In order to increase security incident awareness to certain levels, content of security education and programs should be enhanced with the findings of this research.

It can be suggested that information security awareness education should be more informative about threat and risk environment and how to protect information and systems against to these threats. Additionally, it is more difficult to learn technical side of security issues and threats for non-IT related employees. However, it is more expectable that they will be better aware of security incidents, when they know threats.

It has been also proven that protection knowledge is an important factor to have a knowledge about security incidents. One should understand the answers of the questions regarding how they protect themselves, why they need to protect themselves, what the risk is, how the threat is occurring. Therefore, using real security issues can be better starting point with teaching protection methods and the nature of threats.

To create more influential content for promoting or training of security awareness, security incidents which are more related to target group can be chosen. For example, for Turkish audiences asking Turkish Republic identity data leakage or widespread power outage in Turkey are suitable as it has been investigated in this study. Moreover, to have more attractive content security incidents about popular people and trends, such as the most popular television series Game of Thrones' new seasons' leakage or iCloud hacking of Hollywood celebrities can be involved to create educational content. Education content can be created as not only a class

course or e-learning, but also poster, pop-up remainder, e-mail which is applied commonly in companies.

6.3 Future studies

With using the consequences of this study's results in especially experience dimension, alternative measurements methods can be produced. For example, magnitude of experience can be also evaluated in breach experience measure. Except only asking the type of security breach, whether victim has a serious damage can be evaluated. In order to improve the results related to protection indicator familiarity measure, this factor can be measured by frequency of having security warnings, notifications and indicators in daily routines of employees.

In this study, security incident awareness measure did not include problems which do not have a direct effect on people and/or companies in Turkey such as data breaches of Target stores in 2013 or Equifax data breach in 2017 (Armerding, 2018). There are many data breaches that gives clue about security incidents of near future among them. Additionally, incidents recently happened has been asked to enable respondents to memorize them easily. There are excluded important incidents that can be called the biggest breach in cyber security history such as Yahoo data breach in 2013 with three billion compromised user accounts (Armerding, 2018). Because it is considered that those can be known by experts or people highly interested in cyber security. To measure different perspectives, different data breach examples can be included in future studies.

APPENDIX A
ENGLISH QUESTIONNAIRE

1. Are you currently working?

- Yes
- No

If the answer of the first question is “yes”

2. How many years you have a working experience?

- Less than 1 year
- 1 – 5 years
- 6 – 10 years
- 11 – 15 years
- 16 – 20 years
- 21 – 25 years
- More than 25 years

If the answer of the first question is “no”

2. How many years you have a working experience?

- I do not have any working experience
- Less than 1 year
- 1 – 5 years
- 6 – 10 years
- 11 – 15 years
- 16 – 20 years
- 21 – 25 years
- More than 25 years

If the answer of the second question is not “I do not have any working experience”

3. What is the sector of the company which you are currently working in? (If you are not currently working, please answer for the longest job which you have stayed at the longest)

- Consulting
- Technology
- Banking
- Telecommunication
- Education
- Public Sector
- Insurance and Retirement
- Industrial Products
- Retail and Consumer Products
- Entertainment and Media
- Automotive
- Healthcare
- Construction
- Energy and Utilities
- Pharmaceutical
- Tourism
- Other

If the answer of the second question is not “I do not have any working experience”

4. What is the size of the company which you are currently working in? (If you are not currently working, please answer for the job which you have stayed at the longest)

- 1 – 20
- 21 – 50
- 51 – 100
- 101 – 500
- 501 – 1000
- More than 1000

If the answer of the second question is not “I do not have any working experience”

5. What is your job area in the company which you are currently working? (If you are not currently working, please answer for the job which you have stayed at the longest)

- Human resources
- Finance and accounting
- Marketing and sales
- Procurement
- Communication
- Law
- Operational functions
- Internal control and compliance
- Information security management
- Software development and business analysis
- Information systems network management
- Information systems infrastructure management
- Technical support and service desk management
- Information technology audit and consulting
- Other

6. Please give the best suitable answer for questions about password management given below.

(1: Strongly disagree, 5: Strongly agree)

- Before leaving in front of my computer/laptop, I first lock my system
- I use different passwords for different software, programs and systems
- To remember my password, I write on a notebook or something on my desk
- I do not share my personal account information with my colleagues

7. Please give the best suitable answer for questions about email service usage given below.

(1: Strongly disagree, 5: Strongly agree)

- Before reading an email, I first check if the subject and the sender make sense.
- Before opening an email attachment, I first check if the filename of the attachment makes sense.
- I exercise caution when I receive an email attachment as it may contain a virus.
- I do not open email attachments if the content of the email looks suspicious.

8. Please give the best suitable answer for questions about information handling given below.

(1: Strongly disagree, 5: Strongly agree)

- I do not leave sensitive material unsecure
- I delete information on USB devices after transferring it
- I pay attention whether data is encrypted in the data transfer platform which has been shared with me by third parties
- I do not share my computer with anybody (family member, colleague or customer)
- I destroy sensitive documents securely
- I do not help people who I do not know to enter my company's building

9. Please mention how effective the given protection methods are to provide information security.

(1: Not fully effective, 5: Fully effective)

- Periodically changing passwords of social media or website accounts
- Having a lock in mobile phones
- Not doing any financial transaction via Internet when having public network connection
- Downloading mobile application only from official publisher
- Keeping virus definitions of antivirus protection software updated
- Not sharing banking information with bank personnel in any situation
- Carrying files and documents including important information with a cover
- Not sharing personal information on social media, even if having only close friends and relatives as a connection on social media
- Not downloading free software via web sites which has normally licensing fee
- Having complicated password of wireless network connection at home
- Having antivirus software in mobile phones
- Using two-way authentication in e-mail service and social media accounts
- Checking which services the application can access before downloading the application
- Safely logging out from e-mail service or social media sites in commonly used PC or laptops

10. Please mention which of threats given below result in identity theft.

(yes, uncertain, no)

- Virus
- Trojan
- Botnet
- Social engineering
- Worm
- Key logger
- Phishing

11. Do you know the difference between virus and worm?

- Yes
- No
- Not sure

12. Do you know the difference between malware and spyware?

- Yes
- No
- Not sure

13. Have you ever experienced unauthorized access to email accounts?

- Yes
- No
- Not sure

14. Have you ever experienced unauthorized access to social media accounts or user account of any website?

- Yes
- No
- Not sure

15. Have you ever experienced virus infection on their PCs/laptops?
- Yes
 - No
 - Not sure
16. Have you ever experienced virus infection on mobile devices?
- Yes
 - No
 - Not sure
17. Have you ever experienced data loss because of ransomware attack?
- Yes
 - No
 - Not sure
18. Have you ever experienced financial fraud as a result of drawn bank account, credit card information out of you?
- Yes
 - No
 - Not sure
19. Have you ever haven a notification about security scanning of downloaded e-mail attachments?
- Yes
 - No
 - Not sure
20. Have you ever haven a notification about security scanning of file downloaded from web site?
- Yes
 - No
 - Not sure
21. Have you ever seen https connection in Internet banking and online shopping web site?
- Yes
 - No
 - Not sure
22. Have you ever haven a certification error warning in Internet browser?
- Yes
 - No
 - Not sure
23. Have you ever haven a network connection warning about having shared wireless?
- Yes
 - No
 - Not sure
24. Have you ever seen an indicator related to powerfulness of password while creating in email service or social media sites?
- Yes
 - No
 - Not sure
25. Have you ever haven an e-mail notification from e-mail services or social media sites for logging in from another device?

- Yes
- No
- Not sure

26. Please mention how well you remember given eight security incidents which have targeted individuals or companies, and occurred recent years.

(1: I do not remember at all, 5: I remember very well)

- In recent years, ransomware has threatened users. This ransomware has encrypted all files in systems after opening the attachment or links within a received e-mail which pretends as if send by GSM operators or Internet service providers.
- Wannacry ransomware has spreaded to 200.000 systems within 3 days in almost 150 countries because of a vulnerability of Microsoft Systems. Especially operations of hospitals, telecommunication companies and automotive sector were highly effected.
- In 2016, identity information of approximately 50 million Turkish Republic citizens have been leaked. Database which includes identity information has been provided in the Internet by hackers. Leaked database has included 46 million 611 thousand 709 citizens' TR identity number, mother and father name, date of birth and residence address.
- Power outage which was occurred across Turkey at the beginning of 2017 has become a controversial issue because of spoken cyber-attack suspicion.
- In August 2017, HBO producer of the most popular television series of recent years Game of Thrones has announced that their 1.5 TB data has been leaked which includes the seventh season of Game of Thrones.
- In December 2016, one of the most leading banks in Turkey has announced that their SWIFT international money transfer system has been cyber attacked.
- Between 2014 and 2017 some Hollywood celebrities' private photographs on iCloud have been hacked and shared publicly on the Internet.
- WPA2 protocol which is the most secure and widespread wireless connection encryption method has been hacked.

27. Please mention your gender?

- Female
- Male

28. Please mention your age?

- Under 20
- 20 – 25
- 26 – 30
- 31 – 35
- 36 – 40
- 41 – 45
- Above 45

29. Please mention your education degree?

- High-school
- Associate degree
- Bachelor degree
- Master degree
- Doctorate degree

30. How long you have been using a smartphone

- I am a non-user
- Less than one year
- 1 – 3 years
- 4 – 6 years
- 7 – 10 years
- More than 10 years

31. How long you have a social media account?

- I don't have any
- Less than one year
- 1 – 3 years
- 4 – 6 years
- 7 – 10 years
- More than 10 years

32. Please mention the operating system of your mobile phone?

- Android
- iOS
- Windows
- Other

33. Which one is the most frequently used Internet browser on mobile phone for you?

- Google Chrome
- Firefox
- Internet Explorer
- Safari
- Other

34. Which one is the most frequently used Internet browser on PC/laptop for you?

- Google Chrome
- Firefox
- Internet Explorer
- Safari
- Other

APPENDIX B
TURKISH QUESTIONNAIRE

Bilgi Güvenliđi Anketi

Sayın Katılımcı,

Bu anket, Bođaziçi Üniversitesi Yönetim Bilişim Sistemleri yüksek lisans öğrencisi Nur Sena Tanrıverdi tarafından, Doç Dr. Bilgin Metin danışmanlığında yürütölen yüksek lisans tez çalışması için hazırlanmıştır.

Anket çalışması ile kurum çalışanlarının bilgi güvenliđi davranışlarını ve geçtiğimiz yıllarda yaşanan bilgi güvenliđi olaylarını bilip bilmemelerini etkileyen faktörlerin belirlenmesi hedeflenmektedir.

Ankete vereceğiniz yanıtlar gizli tutulacak olup, sadece akademik amaçlı kullanılacaktır. Anketi yanıtladığınız sırasında sizden kimlik ve iletişim bilgileriniz istenmeyecektir. Anketin tamamlanması en fazla 10 dakika sürmektedir.

İlginiz ve katılımınız için teşekkür ederiz.

Nur Sena Tanrıverdi, Bilgin Metin

[]Mevcut durumda bir kurumda çalışıyor musunuz? *

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır

Kaç yıllık çalışma deneyiminiz bulunuyor?

*

Bunu, yalnızca aşağıdaki koşullar sağlanıyorsa yanıtlayın:

Yanıt şöyleydi: 'Evet' şu soruda: '1 [E1]' (Mevcut durumda bir kurumda çalışıyor musunuz?)

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- 1 yıldan az
 1-5 yıl
 6-10 yıl
 11-15 yıl
 16-20 yıl
 21-25 yıl
 25 yıldan fazla

Kaç yıllık çalışma deneyiminiz bulunuyor?

*

Bunu, yalnızca aşağıdaki koşullar sağlanıyorsa yanıtlayın:

Yanıt şöyleydi: 'Evet' şu soruda: '1 [E1]' (Mevcut durumda bir kurumda çalışıyor musunuz?)

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- 1 yıldan az
- 1-5 yıl
- 6-10 yıl
- 11-15 yıl
- 16-20 yıl
- 21-25 yıl
- 25 yıldan fazla

Çalıştığınız kurumun faaliyet gösterdiği sektörü belirtiniz.

Mevcut durumda çalışmıyor iseniz daha önce en uzun çalıştığınız kurum için soruyu yanıtlandırabilirsiniz.

*

Bunu, yalnızca aşağıdaki koşullar sağlanıyorsa yanıtlayın:

Yanıt şu DEĞİL ise 'Çalışma deneyimim bulunmuyor' şu soruda: '3 [C2]' (Kaç yıllık çalışma deneyiminiz bulunuyor?)

Aşağıdaki yanıtlardan birini seçin

'Diğer:' seçerseniz lütfen seçiminizi uygun metin alanında da belirtin.

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Otomotiv
- Sağlık
- Eğitim
- Teknoloji
- Telekomünikasyon
- Bankacılık ve sermaye piyasaları
- Sigortacılık ve bireysel emeklilik
- Enerji ve altyapı hizmetleri
- Madencilik
- İlaç
- Eğlence ve medya
- Turizm
- Taşımacılık ve lojistik
- Perakende ve tüketici ürünleri
- Varlık ve servet yönetimi
- Gayrimenkul
- Endüstriyel ürünler (kimyasal maddeler, orman ve kağıt ürünleri, inşaat ve yapı, metal)
- Kamu hizmetleri
- Diğer

Çalıştığınız kurumda yaklaşık kaç kişinin çalıştığını belirtiniz.

Mevcut durumda çalışmıyor iseniz daha önce en uzun çalıştığınız kurum için soruyu yanıtlandırabilirsiniz.

*

Bunu, yalnızca aşağıdaki koşullar sağlanıyorsa yanıtlayın:

Yanıt şu DEĞİL ise 'Çalışma deneyimim bulunmuyor' şu soruda: '3 [C2]' (Kaç yıllık çalışma deneyiminiz bulunuyor?)

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- 1-20
- 21-50
- 51-100
- 101-500
- 501-1000
- 1000'den fazla

Çalıştığınız kurumda sorumlu olduğunuz işin konusunu belirtiniz.

Mevcut durumda çalışmıyor iseniz daha önce en uzun çalıştığınız kurum için soruyu yanıtlandırabilirsiniz.

*

Bunu, yalnızca aşağıdaki koşullar sağlanıyorsa yanıtlayın:

Yanıt şu DEĞİL ise 'Çalışma deneyimim bulunmuyor' şu soruda: '3 [C2]' (Kaç yıllık çalışma deneyiminiz bulunuyor?)

Aşağıdaki yanıtlardan birini seçin

'Diğer:' seçerseniz lütfen seçiminizi uygun metin alanında da belirtin.

Lütfen aşağıdakilerden **yalnız birini** seçin:

- İnsan kaynakları
- Finans ve muhasebe
- Pazarlama ve satış
- Satın alma
- İletişim (iç ve dış müşteri, basın)
- Hukuk
- Operasyonel birimler
- İç control, teftiş ve yasal uyum
- Bilgi güvenliği yönetimi
- Yazılım geliştirme ve iş analizi
- Bilgi sistemleri ağ yönetimi
- Bilgi sistemleri altyapı yönetimi
- Teknik destek ve servis masası yönetimi
- Bilgi teknolojileri denetimi ve danışmanlığı
- Diğer

Aşağıda verilen parola yönetimi ile ilgili sorulara sizin için en uygun cevabı veriniz.

(1: Kesinlikle katılmıyorum, 5: Tamamen Katılıyorum)

*

Lütfen her öge için uygun yanıtları seçin:

	1	2	3	4	5
İş yerinde bilgisayarımın önünden kalkmadan önce sistemimi kilitletim	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Çalıştığım kurum tarafından sağlanan bilgisayarda kullandığım farklı uygulama, sistem ve kullanıcı hesapları için farklı parolalar belirlerim	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Parolalarımı, hatırlamak için iş yerinde çalışma masamın üzerinde bir yere veya bir deftere not ederim	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kişisel kullanımında olan kullanıcı hesaplarımın parolalarını çalışma arkadaşlarımla paylaşmam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Aşağıda verilen çalıştığınız kurumdaki e-posta servisi kullanımınız ile ilgili sorulara sizin için en uygun cevabı veriniz.

(1: Kesinlikle katılmıyorum, 5: Tamamen Katılıyorum)

*

Lütfen her öge için uygun yanıtları seçin:

	1	2	3	4	5
Posta kutuma ulaşan bir e-postayı açmadan önce e-postayı gönderenin ve e-postanın konusunun ilgili olup olmadığına bakarım	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Posta kutuma ulaşan bir e-postanın eklerinde bulunan dosyaları indirmeden önce dosya isimlerinin ilgili olup olmadığına bakarım	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
E-postanın ekindeki dosyaların virüs içerme ihtimaline dikkat ederim	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
E-posta içeriğini şüpheli bulursam e-posta eklerini açmam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Aşağıda verilen bilgi kullanımı ile ilgili sorulara sizin için en uygun cevabı veriniz.

(1: Kesinlikle katılmıyorum, 5: Tamamen Katılıyorum)

*

Lütfen her öge için uygun yanıtları seçin:

	1	2	3	4	5
Çalıştığım kurum için hassas ve gizli bilgi içeren materyali (doküman, CD/DVD vb.) üçüncü kişilerce erişimi kolay bir yerde bırakmam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
USB, harici depolama aracı gibi bir elektronik medya aracılığı ile aktarımını yaptığım bilgileri, aktarım yaptıktan hemen sonra ilgili medya üzerinden kaldırırım	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dosya transferi için üçüncü kişiler (ortak iş yapılan kurum dışından kişiler gibi) tarafından sağlanmış dosya aktarım aracının transfer edilen dosyayı şifreleyip şifrelemediğine dikkat ederim	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Çalıştığım kurum tarafından temin edilen bilgisayarımın başkaları (aile üyeleri, iş arkadaşları, müşteriler, arkadaşlar vs.) tarafından kullanımına izin vermem	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Çalıştığım kurum ile ilgili kullanmadığım basılı materyalin güvenli olarak imhasını sağlarım (öğütücüden geçirmek gibi)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tanımadığım kişilerin çalıştığım kuruma fiziksel erişimleri için yardımcı olmam (şahsi kapı kartı vb. ile erişim sağlamak gibi)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Aşağıda verilen koruma yöntemlerinin kişilerin bilgi güvenliğini sağlamakta ne kadar etkili olduğunu belirtiniz.

[]

Aşağıda verilen koruma yöntemlerinin kişilerin bilgi güvenliğini sağlamakta ne kadar etkili olduğunu belirtiniz.

(1: Hiç etkili değildir, 5: Çok etkilidir)

*

Lütfen her öge için uygun yanıtları seçin:

	1	2	3	4	5
İnternet üzerindeki farklı kullanıcı hesaplarının ve sosyal medya hesaplarının şifrelerinin üç ayda bir veya daha sık değiştirilmesi	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cep telefonlarının parola ile kilitletmesi	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
AVM, kafe, restoran gibi kamuya açık alanlarda kablosuz ortak ağlara bağlanıldığında herhangi bir finansal işlem (bankacılık işlemleri, ödeme işlemleri, kredi veya banka kartı ile satın alma işlemleri gibi) yapılmaması	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Akıllı telefon ve tabletlerde yalnızca resmi yayıncısı tarafından paylaşılan uygulamaların kullanılması	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bilgisayarda yüklü antivirüs uygulamasının virus tanımlarının güncel olması	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kişilerin banka kartı ve kredi kartı şifrelerinin hiçbir durumda banka personeli ile paylaşılması	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kişisel bilgi içeren bir evrağı, evrağın üzerindeki bilgilerin görünmeyeceğı şekilde taşınması	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Yakın çevreye (arkadaş ve yakın akrabadan oluşan) hitap ediliyor olursa bile sosyal medya üzerinde özel ve kişisel bilgilerin paylaşılması	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lisans ücreti olan yazılımları ücretsiz olarak sağlayabilen sitelerden bu yazılımları indirmemek	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Evde bulunan kablosuz ağın şifresinin karmaşık bir şifre şeklinde oluşturulması	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobil cihazda antivirüs uygulaması kullanılması	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
E-posta servis hesaplarında ve/veya sosyal medya hesaplarında iki adımlı doğrulama kullanılması	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobil cihaza uygulama indirirken uygulamanın eriştiğı alanlara dikkat edilmesi	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Birden fazla kişinin erişim sağladığı bilgisayarlarda e-posta servisi, sosyal medya siteleri gibi internet sitelerinde açılan kişisel oturumun güvenli olarak kapatılması	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Önemli bilgi ve belgelerin yedeğinin alınması	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Aşağıda verilen daha önce yaşadığınız bilgi güvenliği olayları ile ilgili sorulara sizin için en uygun cevabı veriniz.

[]

E-posta hesaplarınıza yetkisiz kişilerce erişildi mi?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır
 Emin değilim

Sosyal medya ve/veya internet sitesi kullanıcı hesaplarınıza yetkisiz kişilerce erişildi mi?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır
 Emin değilim

Bilgisayarınıza virüs bulaştı mı?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır
 Emin değilim

[]

Mobil cihazınıza virüs bulaştı mı?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır
 Emin değilim

[]

Bilgisayarınızda bulunan, çalışmalarınızda kullandığınız ve/veya arşivlediğiniz fotoğraf, doküman, müzik vb. dosyalarınızın casus yazılımlar ile kilitlenmesi sonucu veri kaybı yaşadınız mı?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır
 Emin değilim

Banka hesap bilgisi, kredi kartı vb. bilgilerinizin sizden alınması ile dolandırıcılığa maruz kaldınız mı?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır
 Emin değilim

Aşağıda verilen daha önce aldığınız güvenlik uyarısı / gördüğünüz güvenlik göstergeleri ile ilgili sorulara sizin için en uygun yanıtı veriniz.

[]

İndirdiğiniz bir e-posta ekinin güvenlik taramasından geçtiğini gördünüz mü?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır
 Emin değilim

[]

İnternet sitesinden indirdiğiniz bir dosyanın güvenlik taramasından geçtiğini gördünüz mü?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır
 Emin değilim

Kullanıcı hesabınız ile giriş yapacağınız bir internet sitesinde, internet sitesinin güvenlik sertifikasına sahip olmaması ile ilgili bir uyarı aldınız mı?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır
 Emin değilim

[]

Müşterisi olduğunuz bankanın internet şubesinin, alışveriş yaptığınız bir sitenin (giyim, ulaşım, yiyecek gibi satın alma yapılan bir site) https bağlantısına sahip olduğunu gördünüz mü?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır
 Emin değilim

Bilgisayar veya mobil cihazınızı ortak bir kablosuz ağına bağlarken ağ bağlantısı ile ilgili bir güvenlik uyarısı aldınız mı?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden yalnız birini seçin:

- Evet
 Hayır
 Emin değilim

[]

E-posta ve/veya sosyal medya hesaplarınızın şifrelerini oluştururken/değiştirirken şifre güvenlik seviyesine yönelik işaretleri (zayıf, orta, güçlü, çok güçlü gibi) gördünüz mü?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden yalnız birini seçin:

- Evet
 Hayır
 Emin değilim

Gmail, Hotmail gibi e-posta hesaplarınıza ve/veya sosyal medya hesaplarınıza farklı cihazlardan erişimleriniz sırasında e-posta veya sms yolu ile "başka bir cihazda oturum açma" ile ilgili bildirim aldınız mı?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden yalnız birini seçin:

- Evet
 Hayır
 Emin değilim

Aşağıda verilen güvenlik tehditleri ile ilgili 3 adet soruyu cevaplandırınız.

[]Aşağıdaki tehditlerden hangisi veya hangileri sonucunda kimlik hırsızlığı gerçekleşebilir? *

Lütfen her öge için uygun yanıtı seçin:

	Evet	Kararsız	Hayır
Virüs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Truva atı	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Botnet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sosyal Mühendislik	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Solucan (worm)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Klavye dinleme (keylogger)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Oltalama (phishing)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

[]

Virüs ile solucan (worm) tehditleri arasındaki farkı biliyor musunuz?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır
 Emin değilim

[]

Kötü amaçlı yazılım (malware) ile casus yazılım (spyware) arasındaki farkı biliyor musunuz?

*

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Evet
 Hayır
 Emin değilim

Aşağıda son yıllarda gerçekleşen, kişi veya kurumları hedef almış 8 adet bilgi güvenliği olayı verilmiştir. Bu olayları hatırlama derecenizi 1'den 5'e kadar değerlendiriniz.

(1: Hiç hatırlamıyorum, 5: Çok iyi hatırlıyorum)

*

Lütfen her öge için uygun yanıtları seçin:

	1	2	3	4	5
Son yıllarda fidye yazılımları (ransomware) tüm internet kullanıcılarını tehdit etti. Bu yazılımlar, GSM operatörleri ve internet sağlayıcıları gibi kurumları taklit ederek oluşturulmuş sahte e-posta hesaplarından kullanıcılara gönderilmiş e-posta ekinin açılması veya e-postada iletilen linkin tıklanması ile bulaşmış ve kullanıcıların bilgisayarlarındaki tüm dosyaları şifreleyerek kullanıcılardan para talep edilmesi ile gerçekleştirilmişti.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2017 Microsoft işletim sistemlerinin bir açığından faydalanarak yayılan WannaCry fidye yazılımı, 3 gün içerisinde 150'ye yakın ülkede 200.000 sisteme bulaştı. Dünya çapında etkili olan bu saldırı	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2016 yılında 50 milyona yakın Türkiye Cumhuriyeti vatandaşının kimlik bilgileri sızdırıldı. Bilgisayar korsanları tarafından T.C. vatandaşlarının kimlik bilgilerinin bulunduğu veritabanı, internet üzerinden paylaşıldı. Sızdırılan veritabanında 2011 seçimi öncesinde seçmen sıfatı kazanmış 46 milyon 611 bin 709 vatandaşın TC kimlik numaraları, anne ve baba isimleri, nüfusa kayıtlı oldukları yer, doğum tarihleri ve MERNİS'e kayıtlı adresleri bulunmaktaydı.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2017 yılının başlarında Türkiye genelinde yaşanan elektrik kesintilerinin siber saldırılardan kaynaklandığı konuşuldu. Benzer şekilde 2015 yılında da 8 saatlik bir elektrik kesintisi yaşanmış, dönemin Enerji ve Tabii Kaynaklar Bakanı siber saldırı olabileceğini belirtmişti. Enerji sektöründe dünya genelinde yaşanan benzer saldırılar, yaşanan elektrik kesintilerinin sebebinin siber saldırı olabileceğini gündeme getirdi.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ağustos 2017'de dünyanın en çok izlenen dizisi Game of Thrones'un yapım şirketi HBO, 7. sezon bölümlerinin de bulunduğu 1.5 TB'lık verilerinin hack'lendiğini duyurdu.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Aralık 2016 tarihinde Türkiye'nin önde gelen bankalarından birinin bilgisayar sistemlerine yönelik bir saldırı gerçekleştirildiği açıklandı. Söz konusu saldırının ülkeler arası para transferini sağlayan SWIFT sistemindeki bir açıktan kaynaklandığı çıkan haberler arasındaydı.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2014 yılında Hollywood ünlülerinin iCloud üzerindeki kişisel fotoğraflarının korsanlar tarafından internette paylaşılması ile gerçekleşen siber güvenlik olayı 2017 yılında farklı ünlülerin hack'lenmesi ile devam etti.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kablosuz internet bağlantılarını şifrelerken kullanılan ve kablosuz bağlantı şifreleme yöntemlerinden en yaygın ve en güvenli olan WPA2 Protokolü'nün hacklendiği açıklandı. KRACK (Key Reinstallation AttaCK) isimli yöntem ile bilgisayar ağlarına sızabilmenin önu açıldı.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

*Yukarıda bahsedilen bilgi güvenliği olayları, bahsi geçen Kurumlar tarafından açıklanmış basında yer alan ve herhangi bir gizliliği olmayan bilgi güvenliği olaylardır.

[]Cinsiyetinizi belirtiniz. *

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Kadın
 Erkek

[]Yaşınızı belirtiniz. *

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- 20 altı
 20-25
 26-30
 31-35
 36-40
 41-45
 45 üzeri

[]Son aldığınız derece itibariyle öğrenim durumunuzu belirtiniz. *

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Lise
 Ön lisans
 Lisans
 Yüksek lisans
 Doktora

[]Kaç yıldır akıllı telefon kullanıyorsunuz? *

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Kullanmıyorum
 1 yıldan az
 1-3 yıl
 4-6 yıl
 7-10 yıl
 10 yıldan fazla

[]Kaç yıldır sosyal medya üzerinde kullanıcı hesabına sahipsiniz? *

Aşağıdaki yanıtlardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Sahip değilim
 1 yıldan az
 1-3 yıl
 4-6 yıl
 7-10 yıl
 10 yıldan fazla

Akıllı telefonunuzun işletim sistemi nedir?

*

Aşağıdaki yanılardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Android
- ios
- Windows
- Diğer (lütfen belirtiniz)

Akıllı telefonunuzda en sık kullandığınız internet tarayıcısı aşağıdakilerden hangisidir lütfen belirtiniz?

*

Aşağıdaki yanılardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Google Chrome
- Firefox
- Internet Explorer
- Safari
- Diğer

[]

Bilgisayarınızda en sık kullandığınız internet tarayıcısı aşağıdakilerden hangisi veya hangileridir lütfen belirtiniz?

*

Aşağıdaki yanılardan birini seçin

Lütfen aşağıdakilerden **yalnız birini** seçin:

- Google Chrome
- Firefox
- Internet Explorer
- Safari
- Diğer

APPENDIX C

DESCRIPTIVE STATISTICS

Table C 1. Descriptive Statistics of First Threat Knowledge Question

Answers	Virus		Trojan		Botnet	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
No	21	6.7	17	5.4	25	7.9
Uncertain	32	10.2	63	20.0	177	56.2
Yes	262	83.2	235	74.6	113	35.9
Total	315	100	315	100	315	100
Answers	Social Engineering		Worm		Key Logger	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
No	24	7.6	25	7.9	11	3.5
Uncertain	110	34.9	105	33.3	57	18.1
Yes	181	57.5	185	58.7	247	78.4
Total	315	100	315	100	315	100
Answers	Phishing					
	Frequency	Percent				
No	4	1.3				
Uncertain	67	21.3				
Yes	244	77.5				
Total	315	100				

Table C 2. Descriptive Statistics of Second and Third Threat Knowledge Question

Answers	Do you know the difference between virus and worm?		Do you know the difference between malware and spyware?	
	Frequency	Percent	Frequency	Percent
Not sure	106	33.7	70	22.2
Yes	101	32.1	83	26.3
No	108	34.3	162	51.4
Total	315	100	315	100

Table C 3. Descriptive Statistics of Breach Experience

Answers	Have you ever experienced unauthorized access to email accounts?		Have you ever experienced unauthorized access to social media accounts or user account of any website?		Have you ever experienced virus infection on their PCs/laptops?	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not sure	30	9.5	27	8.6	23	7.3
Yes	21	6.7	28	8.9	202	64.1
No	264	83.8	260	82.5	90	28.6
Total	315	100	315	100	315	100
Answers	Have you ever experienced virus infection on mobile devices?		Have you ever experienced data loss because of ransomware attack?		Have you ever experienced financial fraud as a result of drawn bank account, credit card information out of you?	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not sure	45	14.3	15	4.8	6	1.9
Yes	19	6.0	35	11.1	33	10.5
No	251	79.7	265	84.1	276	87.6
Total	315	100	315	100	315	100

Table C 4. Descriptive Statistics of Protection Indicator Familiarity

Answers	Have you ever haven a notification about security scanning of downloaded e-mail attachments?		Have you ever haven a notification about security scanning of file downloaded from web site?		Have you ever seen https connection in Internet banking and online shopping web site?	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not sure	31	9.8	25	7.9	29	9.2
Yes	252	80.0	256	81.3	242	76.8
No	32	10.2	34	10.8	44	14.0
Total	315	100	315	100	315	100
Answers	Have you ever haven a certification error warning in Internet browser?		Have you ever haven a network connection warning about having shared wireless?		Have you ever seen an indicator related to powerfulness of password while creating in email service or social media sites?	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not sure	47	14.9	27	8.6	11	3.5
Yes	243	77.1	239	75.9	294	93.3
No	25	7.9	49	15.6	10	3.2
Total	315	100	315	100	315	100
Answers	Have you ever haven an e-mail notification from e-mail services or social media sites for logging in from another device?					
	Frequency	Percent				
Not sure	8	2.5				
Yes	289	91.7				
No	18	5.7				
Total	315	100				

APPENDIX D

RELIABILITY TEST RESULTS

Table D 1. Reliability Statistics of Protection Knowledge

Cronbach's Alpha	N of Items
0.889	15

Table D 2. Item-Total Statistics of Protection Knowledge

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
ProtectionKnowledge_1	58.95	72.688	0.460	0.887
ProtectionKnowledge_2	58.50	74.053	0.525	0.883
ProtectionKnowledge_3	58.55	73.357	0.543	0.882
ProtectionKnowledge_4	58.68	71.415	0.635	0.878
ProtectionKnowledge_5	58.61	71.633	0.627	0.878
ProtectionKnowledge_6	58.23	74.209	0.598	0.880
ProtectionKnowledge_7	58.39	73.532	0.650	0.879
ProtectionKnowledge_8	58.65	73.966	0.476	0.885
ProtectionKnowledge_9	58.98	71.586	0.525	0.883
ProtectionKnowledge_10	58.59	72.363	0.595	0.880
ProtectionKnowledge_11	59.25	70.239	0.560	0.882
ProtectionKnowledge_12	58.60	73.234	0.549	0.882
ProtectionKnowledge_13	58.63	71.082	0.658	0.877
ProtectionKnowledge_14	58.31	74.877	0.613	0.880
ProtectionKnowledge_15	58.40	76.050	0.411	0.887

Table D 3. Reliability Statistics of Security Incident Awareness

Cronbach's Alpha	N of Items
0.813	8

Table D 4. Item-Total Statistics of Security Incident Awareness

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
SecurityIncidentAwareness_1	25.75	44.935	0.561	0.787
SecurityIncidentAwareness_2	25.97	43.805	0.557	0.787
SecurityIncidentAwareness_3	25.1	47.386	0.559	0.789
SecurityIncidentAwareness_4	25.36	46.843	0.532	0.791
SecurityIncidentAwareness_5	25.38	45.402	0.503	0.795
SecurityIncidentAwareness_6	25.88	44.945	0.541	0.790
SecurityIncidentAwareness_7	25.25	47.005	0.516	0.793
SecurityIncidentAwareness_8	26.65	45.235	0.483	0.799

Table D 5. Reliability Statistics of Information Security Behavior

Cronbach's Alpha	N of Items
0.822	14

Table D 6. Item-Total Statistics of Information Security Behavior

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
InformationHandling_1	54.3048	58.232	0.504	0.808
InformationHandling_2	54.9524	56.447	0.472	0.809
InformationHandling_3	55.3714	55.164	0.513	0.806
InformationHandling_4	54.7429	56.077	0.524	0.805
InformationHandling_5	54.7905	55.625	0.52	0.805
InformationHandling_6	54.4159	58.174	0.457	0.81
PasswordManagement_1	54.419	57.569	0.451	0.811
PasswordManagement_2	55.0508	58.138	0.323	0.822
PasswordManagement_3_recode	54.4349	59.68	0.256	0.826
PasswordManagement_4	54.4571	56.587	0.466	0.81
EmailUsage_1	54.4222	58.391	0.476	0.809
EmailUsage_2	54.5397	58.243	0.483	0.809
EmailUsage_3	54.5619	57.323	0.488	0.808
EmailUsage_4	54.1841	59.902	0.468	0.811

APPENDIX E

LINEARITY ASSUMPTION TEST RESULTS

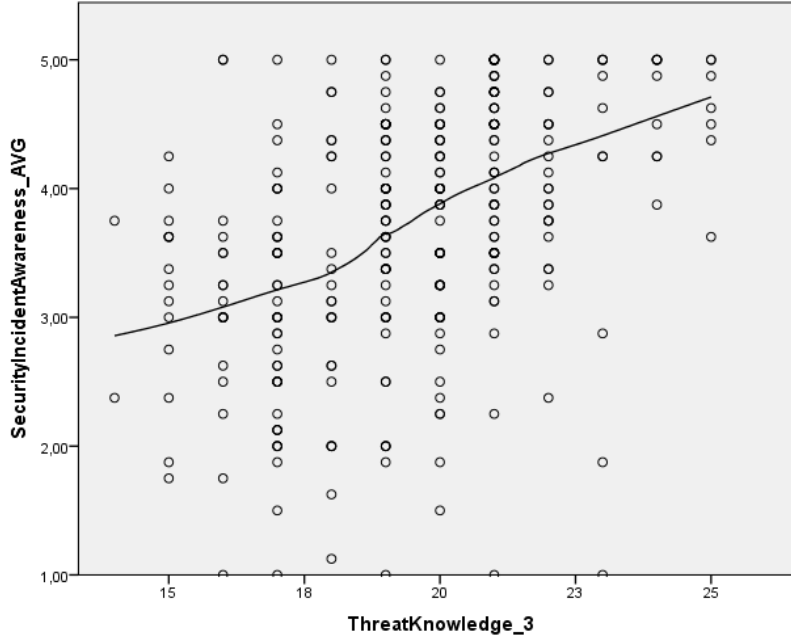


Figure E 1. Linearity check for threat knowledge

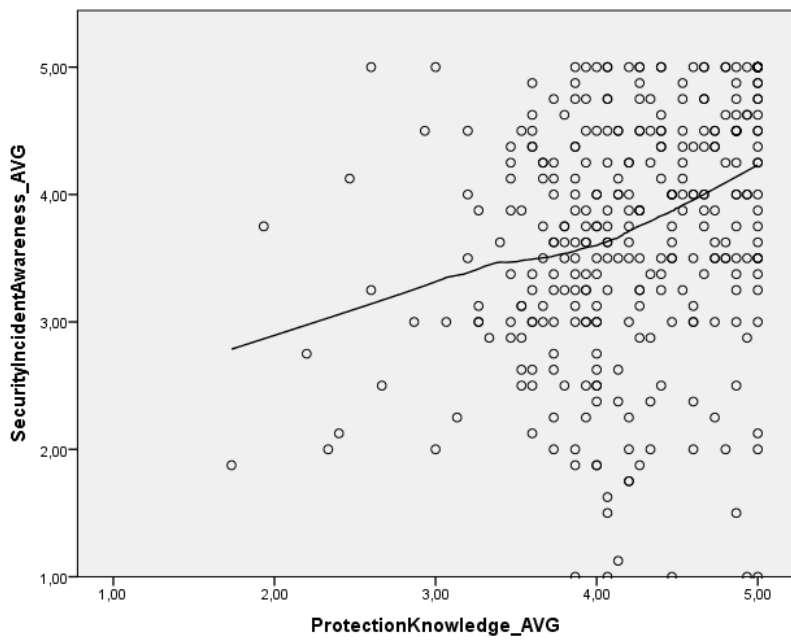


Figure E 2. Linearity check for protection knowledge

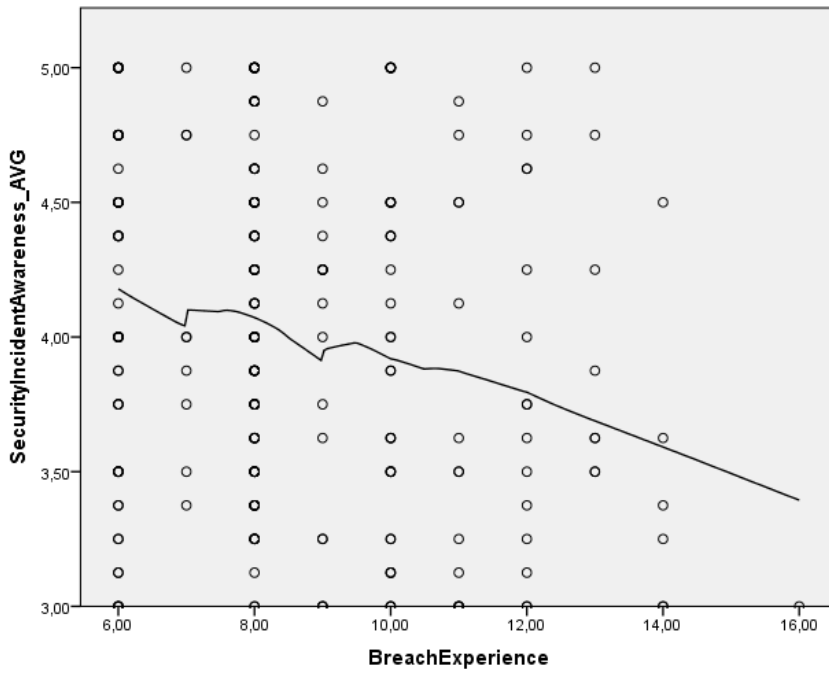


Figure E 3. Linearity check for breach experience

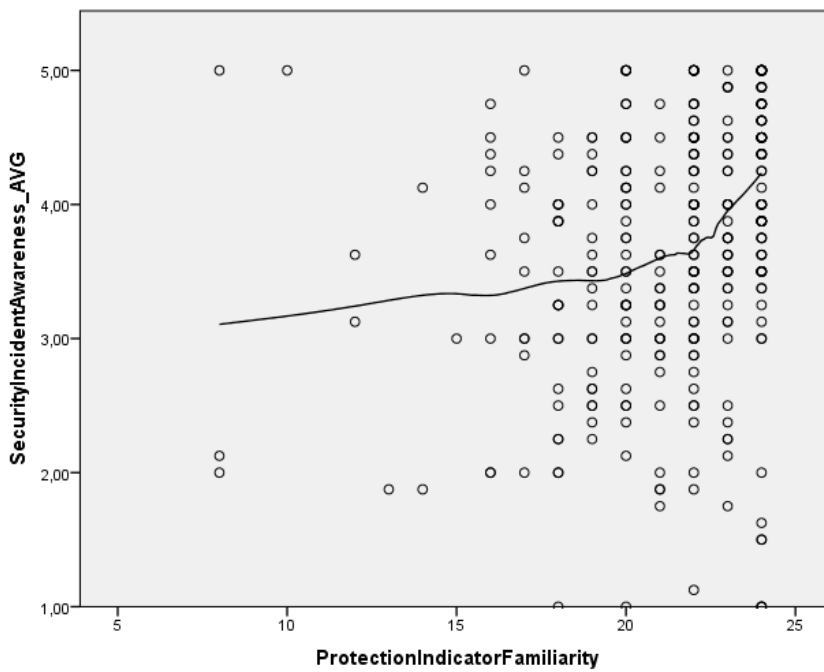


Figure E 4. Linearity check for protection indicator familiarity

APPENDIX F

MULTIPLE REGRESSION TEST RESULTS

Table F 1. Descriptive Statistics

	Mean	Std. Deviation	N
SecurityIncident Awareness_AVG	3,6667	,95302	315
ThreatKnowledge	19,45	2,321	315
ProtectionKnowledge_AVG	4,1873	,60767	315
BreachExperience	8,61	2,100	315
ProtectionIndicatorFamiliarity	21,22	2,891	315

Table F 2. Model Summary^c

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,438 ^a	,192	,189	,85810
2	,468 ^b	,219	,214	,84494

a. Predictors: (Constant), ThreatKnowledge

b. Predictors: (Constant), ThreatKnowledge, ProtectionKnowledge_AVG

c. Dependent Variable: SecurityIncidentAwareness_AVG

Table F 3. ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	54,713	1	54,713	74,304	,000 ^b
	Residual	230,475	313	,736		
	Total	285,188	314			
2	Regression	62,442	2	31,221	43,732	,000 ^c
	Residual	222,745	312	,714		
	Total	285,188	314			

a. Dependent Variable: SecurityIncidentAwareness_AVG

b. Predictors: (Constant), ThreatKnowledge

c. Predictors: (Constant), ThreatKnowledge, ProtectionKnowledge_AVG

Table F 4. Correlations

	SecurityIncidentAwareness_AVG	ThreatKnowledge	Protection Knowledge_AVG	BreachExperience	ProtectionIndicator Familiarity
Pearson Correlation	SecurityIncidentAwareness_AVG	,438	,247	,133	,229
	ThreatKnowledge	1,000	,195	,081	,253
	ProtectionKnowledge_AVG	,247	1,000	,176	,275
	BreachExperience	-,133	-,081	1,000	-,036
	ProtectionIndicatorFamiliarity	,229	,253	,275	1,000
	SecurityIncidentAwareness_AVG	.	,000	,009	,000
	ThreatKnowledge	,000	.	,076	,000
	ProtectionKnowledge_AVG	,000	,000	.	,000
	BreachExperience	,009	,076	,001	,262
	ProtectionIndicatorFamiliarity	,000	,000	,000	.
N	SecurityIncidentAwareness_AVG	315	315	315	315
	ThreatKnowledge	315	315	315	315
	ProtectionKnowledge_AVG	315	315	315	315
	BreachExperience	315	315	315	315
	ProtectionIndicatorFamiliarity	315	315	315	315

Table F 5. Coefficients^a

Model	Unstandardized Coefficients		Standardized Coefficients		t	Sig.	Correlations			Collinearity Statistics	
	B	Std. Error	Beta				Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	,169	,409		,415	,679					
	ThreatKnowledge	,180	,021	,438	8,620	,000	,438	,438	1,000	1,000	
2	(Constant)	-,671	,477		-1,408	,160					
	ThreatKnowledge	,166	,021	,405	7,944	,000	,438	,410	,962	1,040	
	ProtectionKnowledge_AVG	,263	,080	,168	3,290	,001	,247	,183	,962	1,040	

a. Dependent Variable: SecurityIncidentAwareness_AVG

Table F 6. Excluded Variables^a

Model	Beta In	t	Sig.	Partial Correlation	Collinearity Statistics		
					Tolerance	VIF	Minimum Tolerance
1	ProtectionKnowledge_AVG	3,290	,001	,183	,962	1,040	,962
	BreachExperience	-1,935	,054	-,109	,993	1,007	,993
	ProtectionIndicatorFamiliarity	2,433	,016	,136	,936	1,068	,936
2	BreachExperience	-1,441	,151	-,081	,967	1,034	,936
	ProtectionIndicatorFamiliarity	,091 ^c	1,724	,086	,883	1,132	,883

a. Dependent Variable: SecurityIncidentAwareness_AVG

b. Predictors in the Model: (Constant), ThreatKnowledge

c. Predictors in the Model: (Constant), ThreatKnowledge, ProtectionKnowledge_AVG

APPENDIX G

DESCRIPTIVE STATISTICS OF 60 RESPONDENTS

Table G 1. Demographics of 60 Respondents

	Variables	Frequency	Percent
Gender	Male	29	48,3
	Female	31	51,7
Age	20-25	15	25,0
	26-30	26	43,3
	31-35	10	16,7
	36-40	6	10,0
	41-45	2	3,3
	Above 45	1	1,7
Education	Doctorate	9	2.9
	Master	69	21.9
	Bachelor	218	69.2
	Associate	10	3.2
	High School	9	2.9
	Total	60	100

Table G 2. Company Information of 60 Respondents

Variables		Frequency	Percentage
Company Size	1-20	7	11,7
	21-50	6	10,0
	101-500	7	11,7
	501-1000	4	6,7
	Above 1000	36	60,0
Company Sector	Consulting	17	28,3
	Banking	4	6,7
	Education	4	6,7
	Entertainment and Media	2	3,3
	Industrial products	1	1,7
	Energy and Utilities	1	1,7
	Pharmaceutical	1	1,7
	Construction	2	3,3
	Public Sector	5	8,3
	Automotive	2	3,3
	Retail and Consumer Products	1	1,7
	Healthcare	2	3,3
	Insurance and Retirement	2	3,3
	Technology	8	13,3
	Telecommunication	6	10,0
Tourism	2	3,3	
Total		60	100,0

Table G 3. Working Information of 60 Respondents

Variables		Frequency	Percent
Working Experience	Below 1 year	5	8,3
	1-5 years	36	60,0
	6-10 years	10	16,7
	11-15 years	2	3,3
	16-20 years	6	10,0
	Above 25 years	1	1,7
Profession	IT Related	22	36,7
	Non-IT Related	36	60,0
	Other	2	3,3
Total		60	100

Table G 4. Technology Usage of 60 Respondents

Variables		Frequency	Percent
Smartphone Usage	1-3 years	14	4,4
	4-6 years	22	36,7
	7-10 years	26	43,3
	Above 10 years	9	15,0
Social Media Usage	Below 1 year	1	1,7
	1-3 years	1	1,7
	4-6 years	8	13,3
	7-10 years	30	50,0
	Above 10 years	18	30,0
Non-user		2	3,3
Operating System of Smartphone	Android	22	36,7
	iOS	37	61,7
	Other	1	1,7
The most used Internet Browser in Smartphone	Firefox	2	3,3
	Google Chrome	25	41,7
	Internet Explorer	2	3,3
	Safari	29	48,3
	Other	2	3,3
The most used Internet Browser in PC/Laptop	Firefox	2	3,3
	Google Chrome	53	88,3
	Internet Explorer	3	5,0
	Safari	1	1,7
	Other	1	1,7
Total		60	100

Table G 5. Descriptive Statistics of Security Behavior

Security Behavior		Mean	Std. Dev.	Min	Max
EmailUsage_1	Before reading an email, I will first check if the subject and the sender make sense.	4.12	1.18	1	5
EmailUsage_2	Before opening an email attachment, I will first check if the filename of the attachment makes sense.	3.98	1.066	1	5
EmailUsage_3	I exercise caution when I receive an email attachment as it may contain a virus.	3.92	1.197	1	5
EmailUsage_4	I do not open email attachments if the content of the email looks suspicious.	4.4	1.012	1	5
Password Management_1	Before leaving in front of my computer/laptop, I will first lock my system	4.15	1.233	1	5
Password Management_2	I use different passwords for different software, programs and systems	3.63	1.327	1	5
Password Management_3_recode	To remember my password, I write on a notebook or something on my desk	4.25	1.257	1	5
Password Management_4	I do not share my personal account information with my colleagues	4.22	1.209	1	5
Information Handling_1	I do not leave sensitive material unsecure	4.38	0.993	1	5
Information Handling_2	I delete information on USB devices after transferring it	3.68	1.242	1	5
Information Handling_3	I pay attention whether data is encrypted in the data transfer platform which has been shared with me by third parties	3.45	1.268	1	5
Information Handling_4	I do not share my computer with anybody (family member, colleague or customer)	3.83	1.167	1	5
Information Handling_5	I destroy sensitive documents securely	3.88	1.209	1	5
Information Handling_6	I do not help people who I do not know to enter my company's building	4.27	1.118	1	5
Security Behavior_AVG	Average Security Behavior	4.01	0.696	1.29	5

APPENDIX H

WLS REGRESSION TEST RESULTS

Table H 1. Descriptive Statistics^a

	Mean	Std. Deviation	N
SecurityBehavior_AVG	4,3315	1,44668	255
SecurityIncidentAwareness_AVG	4,2376	1,73483	255

a. Weighted Least Squares Regression - Weighted by weight_9

Table H 2. Correlations^a

		Security Behavior_AVG	SecurityIncident Awareness_AVG
Pearson Correlation	SecurityBehavior_AVG	1,000	,474
	SecurityIncidentAwareness_AVG	,474	1,000
Sig. (1-tailed)	SecurityBehavior_AVG	.	,000
	SecurityIncidentAwareness_AVG	,000	.
N	SecurityBehavior_AVG	255	255
	SecurityIncidentAwareness_AVG	255	255

a. Weighted Least Squares Regression - Weighted by weight_9

Table H 3. Variables Entered/Removed^{a,b}

Model	Variables Entered	Variables Removed	Method
1	SecurityIncidentAwareness_AVG ^c	.	Enter

a. Dependent Variable: SecurityBehavior_AVG

b. Weighted Least Squares Regression - Weighted by weight_9

c. All requested variables entered.

Table H 4. Model Summary^{b,c}

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,474 ^a	,224	,221	1,27652

a. Predictors: (Constant), SecurityIncidentAwareness_AVG

b. Dependent Variable: SecurityBehavior_AVG

c. Weighted Least Squares Regression - Weighted by weight_9

Table H 5. ANOVA^{a,b}

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	119,328	1	119,328	73,230	,000 ^c
	Residual	412,266	253	1,630		
	Total	531,594	254			

a. Dependent Variable: SecurityBehavior_AVG

b. Weighted Least Squares Regression - Weighted by weight_9

c. Predictors: (Constant), SecurityIncidentAwareness_AVG

Table H 6. Collinearity Diagnostics^{a,b}

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions	
				(Constant)	SecurityIncident Awareness_AVG
1	1	1,990	1,000	,01	,01
	2	,010	13,812	,99	,99

a. Dependent Variable: SecurityBehavior_AVG

b. Weighted Least Squares Regression - Weighted by weight_9

Table H 7. Coefficients^{a,b}

Model	Unstandardized Coefficients		Standardized Coefficients		t	Sig.	Correlations			Collinearity Statistics	
	B	Std. Error	Beta	Zero-order			Partial	Part	Tolerance	VIF	
											B
1											
	(Constant)	2,657	,198		13,440	,000					
	SecurityIncident	,395	,046	,474	8,557	,000	,474	,474	,474	1,000	1,000
	Awareness_AVG										

a. Dependent Variable: SecurityBehavior_AVG

b. Weighted Least Squares Regression - Weighted by weight_9

Table H 8. Residual Statistics^{a,b}

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	3,8425	4,6327	4,2456	,24984	255
Residual	-2,12824	,88850	,00038	,48111	255
Std. Predicted Value ^c	0
Std. Residual ^c	0

a. Dependent Variable: SecurityBehavior_AVG

b. Weighted Least Squares Regression - Weighted by weight_9

c. Not computed for Weighted Least Squares regression.

APPENDIX I

ADDITIONAL ANALYSES: MULTIPLE REGRESSION TEST OF PART 1

AFTER EXCLUDING 60 RESPONSES

Table I 1. Descriptive Statistics

	Mean	Std. Deviation	N
SecurityIncidentAwareness_AVG	4,0201	,63236	255
ThreatKnowledge	19,76	2,273	255
BreachExperience	8,59	2,137	255
ProtectionIndicatorFamiliarity	21,50	2,697	255
ProtectionKnowledge_AVG	4,2431	,57236	255

Table I 2. Correlations

	SecurityIncidentAwareness_AVG	ThreatKnowledge	BreachExperience	SecurityProtectionIndicator	ProtectionKnowledge_AVG
Pearson Correlation	SecurityIncidentAwareness_AVG	,438	,202	,180	,255
	ThreatKnowledge	1,000	,109	,303	,187
	BreachExperience	-,202	1,000	-,073	-,179
	ProtectionIndicatorFamiliarity	,180	-,109	1,000	,289
	ProtectionKnowledge_AVG	,255	,303	,073	1,000
	SecurityIncidentAwareness_AVG	.	,187	,179	,289
Sig. (1-tailed)	ThreatKnowledge	,000	,001	,002	,000
	BreachExperience	,001	,042	,000	,001
	ProtectionIndicatorFamiliarity	,002	,042	,124	,002
	ProtectionKnowledge_AVG	,000	,000	,124	,000
	SecurityIncidentAwareness_AVG	255	255	,002	,000
	ThreatKnowledge	255	255	255	255
N	BreachExperience	255	255	255	255
	ProtectionIndicatorFamiliarity	255	255	255	255
	ProtectionKnowledge_AVG	255	255	255	255
	SecurityIncidentAwareness_AVG	255	255	255	255
	ThreatKnowledge	255	255	255	255
	BreachExperience	255	255	255	255

Table I 3. Model Summary^d

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,438 ^a	,192	,188	,56965
2	,472 ^b	,223	,217	,55970
3	,489 ^c	,239	,230	,55485

a. Predictors: (Constant), ThreatKnowledge

b. Predictors: (Constant), ThreatKnowledge, ProtectionKnowledge_AVG

c. Predictors: (Constant), ThreatKnowledge, ProtectionKnowledge_AVG, BreachExperience

d. Dependent Variable: SecurityIncidentAwareness_AVG

Table I 4. ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	19,470	1	19,470	59,999	,000 ^b
	Residual	82,099	253	,325		
	Total	101,569	254			
2	Regression	22,627	2	11,314	36,116	,000 ^c
	Residual	78,942	252	,313		
	Total	101,569	254			
3	Regression	24,297	3	8,099	26,308	,000 ^d
	Residual	77,272	251	,308		
	Total	101,569	254			

a. Dependent Variable: SecurityIncidentAwareness_AVG

b. Predictors: (Constant), ThreatKnowledge

c. Predictors: (Constant), ThreatKnowledge, ProtectionKnowledge_AVG

d. Predictors: (Constant), ThreatKnowledge, ProtectionKnowledge_AVG, BreachExperience

Table I 5. Coefficients^a

Model	Unstandardized Coefficients			Standardized Coefficients		T	Sig.	Correlations			Collinearity Statistics	
	B	Std. Error	Beta		Beta			Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	1,613	,313			5,158	,000					
	ThreatKnowledge	,122	,016	,438		7,746	,000	,438	,438	,438	1,000	1,000
2	(Constant)	,956	,370			2,582	,010					
	ThreatKnowledge	,112	,016	,404		7,150	,000	,438	,411	,397	,965	1,036
	ProtectionKnowledge_AVG	,198	,062	,179		3,175	,002	,255	,196	,176	,965	1,036
3	(Constant)	,517	,413			1,252	,212					
	ThreatKnowledge	,110	,016	,394		7,010	,000	,438	,405	,386	,959	1,043
	ProtectionKnowledge_AVG	,175	,063	,158		2,782	,006	,255	,173	,153	,940	1,064
	BreachExperience	-,039	,017	-,131		-2,329	,021	-,202	-,145	-,128	,962	1,039

a. Dependent Variable: SecurityIncidentAwareness_AVG

Table I 6. Excluded Variables^a

Model	Beta In	t	Sig.	Partial Correlation	Collinearity Statistics		
					Tolerance	VIF	Minimum Tolerance
1	BreachExperience	-2,781	,006	-,173	,988	1,012	,988
	ProtectionIndicatorFamiliarity	,878	,381	,055	,908	1,101	,908
	ProtectionKnowledge_AVG	3,175	,002	,196	,965	1,036	,965
2	BreachExperience	-2,329	,021	-,145	,962	1,039	,940
	ProtectionIndicatorFamiliarity	,110	,913	,007	,852	1,174	,852
3	ProtectionIndicatorFamiliarity	,107	,915	,007	,852	1,174	,852

a. Dependent Variable: SecurityIncidentAwareness_AVG

b. Predictors in the Model: (Constant), ThreatKnowledge

c. Predictors in the Model: (Constant), ThreatKnowledge, ProtectionKnowledge_AVG

d. Predictors in the Model: (Constant), ThreatKnowledge, ProtectionKnowledge_AVG, BreachExperience

APPENDIX J

ADDITIONAL ANALYSES: PROFESSION DIFFERENCE WITH RESPECT TO THREAT KNOWLEDGE AND PROTECTION KNOWLEDGE

Table J 1. Group Statistics

	Profession	N	Mean	Std. Deviation	Std. Error Mean
ThreatKnowledge	IT	162	20,20	2,144	,168
	Non-IT	145	18,62	2,276	,189

Table J 2. Independent Samples Test

Threat Knowledge		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
Threat Knowledge	Equal variances assumed	,631	,428	6,272	305	,000	1,583	,252	Lower 1,086	Upper 2,080
	Equal variances not assumed			6,252	296,368	,000	1,583	,253	Lower 1,085	Upper 2,081

Table J 3. Group Statistics

	Profession	N	Mean	Std. Deviation	Std. Error Mean
ProtectionKnowledge_AVG	IT	162	4,2399	,55233	,04339
	Non-IT	145	4,1126	,66274	,05504

Table J 4. Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
Protection Knowledge_AVG		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Protection Knowledge_AVG	Equal variances assumed	2,072	,151	1,834	305	,068	,12727	,06939	-,00927	,26382
	Equal variances not assumed			1,816	281,416	,070	,12727	,07009	-,01069	,26524

APPENDIX K

ADDITIONAL ANALYSES: GENDER DIFFERENCE

WITH RESPECT TO SECURITY INCIDENT AWARENESS AND SECURITY BEHAVIOR

Table K 1. Group Statistics

	Gender	N	Mean	Std. Deviation	Std. Error Mean
SecurityIncidentAwareness_AVG	Female	137	3,4115	,86232	,07367
	Male	178	3,8631	,97503	,07308

Table K 2. Independent Samples Test

SecurityIncident Awareness_AVG		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
	Equal variances assumed	3,226	,073	-4,283	313	,000	-,45157	,10544	-,65903	-,24410
	Equal variances not assumed			-4,352	306,961	,000	-,45157	,10377	-,65576	-,24737

Table K 3. Group Statistics

	Gender	N	Mean	Std. Deviation	Std. Error Mean
SecurityBehavior_AVG	Female	137	4,1632	,53283	,04552
	Male	178	4,2307	,61294	,04594

Table K 4. Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
SecurityBehavior_AVG	Equal variances assumed	,113	,737	-1,026	313	,306	-,06755	,06586	-,19714	,06204
	Equal variances not assumed			-1,044	308,343	,297	-,06755	,06468	-,19481	,05971

REFERENCES

- Abraham, S. (2011). Information security behavior: Factors and research directions. *Proceedings of The Seventeenth Americas Conference on Information Systems* (p. 462). Detroit, Michigan.
- Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Information security policy compliance: The role of information security awareness. *Proceedings of the American Conference on Information Systems*. Seattle, Washington.
- AlKalbani, A., Deng, H., & Kam, B. (2015). Organizational security culture and information security compliance for e-government development: The moderating effect of social pressure. *Pacific Asia Conference on Information Systems 2015*. Marina Bay Sands, Singapore.
- Apple. (n.d.1). *Here's how to manage your privacy*. Retrieved from <https://www.apple.com/privacy/manage-your-privacy/>
- Apple (n.d.2). *Do I need antivirus software for my iPhone?* Retrieved from <https://www.apple.com/shop/question/answers/iphone/do-i-need-antivirus-software-for-my-iphone/Q2JF22AYP7YY7DHKT>
- Armerding, T. (2018, January 26). The 17 biggest data breaches of the 21st century. *CSO Online*. Retrieved from <https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html>
- Beyhan, T. (2017, October 16). Kablosuz internet kullanıcıları tehlikede; şifrelemede kullanılan WPA2 protokolü hacklendi. *T24*. Retrieved from http://t24.com.tr/haber/kablosuz-internet-kullanicilari-tehlikede-sifrelemede-kullanilan-wpa2-protokolu-hacklendi,465858?lipi=urn%3Ali%3Apage%3Ad_flagship3_feed%3BtAbQ02j%2BSF68%2By3hPUs2Hw%3D%3D
- Bhattacharjee, A., & Hikmet, N. (2007). A physicians' resistance toward healthcare information technology: A theoretical model and empirical test. *European Journal of Information Systems*, 16(2007), 725-737. doi:10.1057/palgrave.ejis.3000717

- 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), 523–548.
- Chen Y, & Zahedi F. M. (2016). Individuals' internet security perceptions and behaviors: Polycontextual. *MIS Quarterly*, 40(1), 205-222.
- Cisco. (n.d.). *What is the difference: Viruses, worms, trojans, and bots?* Retrieved from <https://www.cisco.com/c/en/us/about/security-center/virus-differences.html>
- Cohen, J., Cohen, P., West, S. G., Aiken, L. S. (2003). *Applied multiple regression/correlation analysis for the behavioral sciences* (3rd ed.). Mahwah, NJ: Lawrence Erlbaum Associates.
- Crowson, H. M. (2015, November 19). Weighted least squares regression using SPSS [Video file]. Retrieved from https://www.youtube.com/watch?v=enPK_SXILnA
- Cummings, J., Gomillion, D., & Connolly, A. J. (2017). Impacts of generational work experience on users' perceptions of information security. *Twenty-third Americas Conference on Information Systems*. Boston, MA.
- CyberMag. (n.d.). *Dünya fidye yazılımına karşı ayakta*. Retrieved from <http://www.cybermagonline.com/dunya-fidye-yazilimina-karsi-ayakta>
- Elçiboğa, İ. K. (2018). *Kartlı ödeme dolandırıcılık türleri, risk ve mali sorumlulukları*. Retrieved from <http://fintechtime.com/tr/2018/02/kartli-odeme-dolandiricilik-turleri-risk-ve-mali-sorumluluklari/>
- Eugdpr.org. (n.d.) *GDPR portal: Site overview*. Retrieved from <https://www.eugdpr.org>
- 50 milyon vatandaşın kimlik bilgileri internette! (2016, April 6). *Sözcü*. Retrieved from <http://www.sozcu.com.tr/2016/gundem/50-milyon-vatandasin-kimlik-bilgileri-internette-1170573/>
- Furnell, S. M., & Karweni, T. (1999). Security implications of electronic commerce: a survey of consumers and businesses. *Internet Research*, 9(5), 372-382. doi: 10.1108/10662249910297778

- Garanti. (n.d.). *Security*. Retrieved from https://www.garanti.com.tr/en/personal_banking/delivery_channels/internet_banking/security.page
- Garg, V., & Camp, J. (2012). End user perception of online risk under uncertainty. *IEEE Computer Society: 2012 45th Hawaii International Conference on System Sciences*. Maui, Hawaii. doi:10.1109/HICSS.2012.245
- Google. (n.d.). *2 adımlı doğrulama*. Retrieved from <https://www.google.com/landing/2step/>
- Gujarati, D. N. (1988). *Basic econometrics* (2nd ed.). Singapore: McGraw-Hill.
- Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior. *Proceedings of the 15th International Conference on Information Systems (ICIS)* (p. 11-49). San Milan, Italy.
- Haeussinger, F., & Kranz, J. (2017). Antecedents of employees' information security awareness - review, synthesis, and directions for future research. Twenty-Fifth European Conference on Information Systems (ECIS). Guimarães, Portugal.
- Hair, J. F., Anderson, R. E, Tatham, R. L., & Black, W. C. (1995). *Multivariate data analysis with readings* (4th ed.). Englewood Cliffs, NJ: Prentice Hall.
- Harding, L. (2016, December 16). What we know about Russia's inference in the US election. *The Guardian*. Retrieved from <https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election>
- Heartfield, R., Loukas, G., & Gan, D. (2016). You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. *IEEE Access*, 4(2016), 6910-6928. doi:10.1109/ACCESS.2016.2616285
- Herath, T., & Rao, H. G. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2), 106-125.
- Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H.R. (2012). Security services as coping mechanisms: An investigation into user intention to adopt an

email authentication service. *Information Systems Journal*, 21(1), 61-84.
doi:10.1111/j.1365-2575.2012.00420.x

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, 49(2), 99-110.

Hu, Q., & 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), 386–408.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The role of top management and organizational culture. *Decision Sciences*, 43(4). doi: 10.1111/j.1540-5915.2012.00361.x

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2007). A survey of factors influencing people's perception of information security. *Human Computer Interaction*, 2(4), 906-915.

IBM Knowledge Center. (n.d.1). *Fit Lines*. Retrieved from https://www.ibm.com/support/knowledgecenter/en/SSLVMB_23.0.0/spss/base/ih_webhelp_fitline_palette.html

IBM Knowledge Center. (n.d.2). *Residual Plots*. Retrieved from https://www.ibm.com/support/knowledgecenter/en/SSLVMB_sub/statistics_case_studies_project_ddita/spss/tutorials/wls_residual-plots.html

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), 83-95. doi:10.1016/j.cose.2011.10.007

Interbank Card Center. (n.d.). *Secure online shopping*. Retrieved from <https://bkm.com.tr/guvenlik-bkm/>

Interbank Card Center Express. (n.d.) *BKM Express güvenlik uyarıları*. Retrieved from <https://bkmexpress.com.tr/guvenlik>

International Organization for Standardization. (2013). *Information technology - Security techniques code of practice for information security controls* (BS ISO/IEC 27002:2013).

- Jaeger, L., Ament, C., & Eckhardt, A. (2017). The closer you get the more aware you become – a case study about psychological distance to information security incidents. *International Conference on Information Systems 2017 Proceedings*. Seoul, Korea.
- Jeske, D., & Schaik, P. V. (2017). Familiarity with threats: Beyond awareness. *Computers & Security*, 66(2017), 129-141. doi:10.1016/j.cose.2017.01.010
- Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1). 113-134. doi:10.25300/MISQ/2015/39.1.06
- Johnston, A.C., Wech, B., Jack, E., & Beavers, M. (2010). Reigning in the remote employee: applying social learning theory to explain information security policy compliance attitudes. *Proceedings of the American Conference on Information Systems* (p. 493). Lima, Peru.
- Jones, R. (2017, August 23). Identity fraud reaching epidemic levels, new figures show. *The Guardian*. Retrieved from <https://www.theguardian.com/money/2017/aug/23/identity-fraud-figures-cifas-theft>
- Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: A contextual perspective. *Computers & Security*, 24(2005), 246-260.
- Kaspersky. (n.d.). *The human factor in IT security: How employees are making businesses vulnerable from within*. Retrieved from <https://www.kaspersky.com/blog/the-human-factor-in-it-security/>
- Kelley, T., & Bertenthal, B. I. (2016). Attention and past behavior, not security knowledge, modulate users' decisions to login to insecure websites. *Information & Computer Security*, 24(2), 164-176. doi:10.1108/ICS-01-2016-0002
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(2006), 289-296.
- KVKP. (2016). *Turkish personal data protection law no. 6698*. Retrieved from <https://www.kisiselverilerinkorunmasi.org/kanunu-ingilizce-ceviri/>

- Laerd Statistics. (2015a). *Multiple regression using SPSS statistics*. Retrieved from <https://statistics.laerd.com/>
- Laerd Statistics. (2015b). *Checking for normality of residuals (errors)*. Retrieved from <https://statistics.laerd.com/premium/spss/lr/linear-regression-in-spss-14.php>
- Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, 37(12), 1049-1092. doi:10.1108/MRR-04-2013-0085
- Limayem, M., & Hirt, S. G. (2003). Force of habit and information systems usage: theory and initial validation. *Journal of Association for Information Systems*, 4(1), 65-97.
- Lomo-David, E., & Shannon, L. J. (2009). Critical analysis of mobile phone communication safety and security measures: Familiarity versus actual practice on mobile devices. *Proc ISECON*, 26(2009), 1-19.
- Luciano, E. M., Mahmood, M. A., & Maçada, A. C. G. (2010). The influence of human factors on vulnerability to information security breaches. Sixteenth Americas Conference on Information Systems. Lima, Peru.
- Ng, B. Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(2009), 815-825. doi:10.1016/j.dss.2008.11.010
- Nishioka, D., Murayama, Y., & Fujihara, Y. (2012). Producing a questionnaire for a user survey on anshin with information security for users without technical knowledge. *IEEE Computer Society: 2012 45th Hawaii International Conference on System Sciences*. Maui, Hawaii. doi:10.1109/HICSS.2012.34
- NTV. (2017). *HBO siber saldırıyı doğruladı: Game of Thrones'un 7. sezonunun senaryosu sızdırıldı*. Retrieved from <https://www.ntv.com.tr/galeri/sanat/hbo-siber-saldiriyi-dogruladi-game-of-thronesun-7-sezonunun-senaryosu-sizdirild,oue3wmBdq0uhN7RD9v7NUQ/xiz21R7aVUG3W6T7Uy1p4A#xiz21R7aVUG3W6T7Uy1p4A>
- Onat, K. (2016). *Cryptolocker virüsü nedir ve nasıl kurtulabiliriz?* Retrieved from <http://www.webtekno.com/internet/cryptolocker-virus-kaldirma-h12016.html>

- Pahnila, S., Siponen, M. T., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences* (pp. 1-10), Big Island, Hawaii.
- Panko, R. R., & Panko, J. L. (2013). *Business data networks and security* (9th ed.). New Jersey: Pearson Education.
- Parsons, K, McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, 42(2014), 165-176. doi:10.1016/j.cose.2013.12.003:
- Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, 20(1). 18-28. doi:10.1108/09685221211219173
- Pindyck, R. S., & Rubinfeld, D. L. (1991). *Econometric models & econometric forecasts* (3rd ed.). Singapore: McGraw-Hill.
- PricewaterhouseCoopers. (2016). Global state of information security survey 2017. Retrieved from <https://www.pwc.com/gsis2017>.
- Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(2009), 816-826. doi:10.1016/j.cose.2009.05.008
- Ross, S. J. (2011). Creating a culture of security. Retrieved from <https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Creating-a-Culture-of-Security.aspx>
- Rughiniş, C., & Rughiniş, R. (2014). Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union. *Computers & Security*, 43(2014), 111-125. doi:10.1016/j.cose.2014.03.008
- Ryan, J. E. (2007). Information security awareness: An evaluation among business students with regard to computer self-efficacy and personal Innovation. *Proceedings of the 9th Americas Conference on Information Systems (AMCIS)* (p. 251). Florida, USA.

- Sezer, C., & Altayli, B. (2016). *Turkey's Akbank faces \$4 million hit from attempted cyber heist*. Retrieved from <https://www.reuters.com/article/us-akbank-cyber/turkeys-akbank-faces-4-million-hit-from-attempted-cyber-heist-idUSKBN1450MC>
- ShiftDelete.Net. (2017). *Emma Watson'in gizli fotoğrafları hacklendi!* Retrieved from <https://shiftdelete.net/emma-watson-da-hack-kurbani-oldu-80232>
- Siponen, M. T., Pahnla, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. *Proceedings of the IFIP SEC* (pp. 133-144). Brisbane, Australia.
- Siponen, M. T., Pahnla, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, 43(2), 64-71.
- Tanriverdi, N. S., & Metin, B. (2017a). Students and information security culture in organizations. *The Eleventh Mediterranean Conference on Information Systems*. Genoa, Italy.
- Tanriverdi, N. S., & Metin, B. (2017b). Evaluation of IT security perception. *Twenty-third Americas Conference on Information Systems* (p. 42). Boston, USA.
- The European Union Agency for Network and Information Security. (2018). *ENISA threat landscape report 2017*. Retrieved from <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017>
- Timmers, C. F., & Glas, C. A. W. (2010). Developing scales for information-seeking behaviour. *Journal of Documentation*, 66(1), 46-69
- 2 yıl önce Türkiye genelinde kesilen elektriğin nedeni İran'ın siber saldırısı mı? (2017, July 14). *T24*. Retrieved from <http://t24.com.tr/haber/2-yil-once-turkiye-genelinde-kesilen-elektrigin-nedeni-iranin-siber-saldirisi-mi,414375>
- Wallen, J. (2016). *Google Chrome security tips for the paranoid at heart*. Retrieved from <https://www.techrepublic.com/article/google-chrome-security-tips-for-the-paranoid-at-heart/>

Yang, R., Ng, Y. J., & Vishwanath, A. (2015). Do social media privacy policies matter evaluating the effects of familiarity and privacy seals on cognitive processing? *IEEE Computer Society: 2015 48th Hawaii International Conference on System Sciences*. Kauai, Hawaii. doi:10.1109/HICSS.2015.417

Zhang, P., & Li, X. (2015). Determinants of information security awareness: An empirical investigation in higher education. *Proceedings of the Thirty Sixth International Conference on Information Systems (ICIS)*. Texas, USA.