"İŞ, GÜÇ" ENDÜSTRİ İLİŞKİLERİ VE İNSAN KAYNAKLARI DERGİSİ

"IS, GUC" Industrial Relations and Human Resources Journal

2020 Cilt/Vol: 22/Num:1 Sayfa/Page: 1-20

ISGUC.ORG

İŞ, GÜÇ ISSN 2148-9874
Endüstri İlişkileri ve İnsan Kaynakları Dergisi

İş,Güç, Endüstri İlişkileri ve İnsan Kaynakları Dergisi, yılda dört kez yayınlanan hakemli, bilimsel elektronik dergidir. Çalışma hayatına ilişkin makalelere yer verilen derginin temel amacı, belirlenen alanda akademik gelişime ve paylaşıma katkıda bulunmaktadır. "İş, Güç," Endüstri İlişkileri ve İnsan Kaynakları Dergisi, 'Türkçe' ve 'İngilizce' olarak iki dilde makale yayınlanmaktadır.

"Is,Guc" The Journal of Industrial Relations and Human Resources is peer-reviewed, quarterly and electronic open sources journal. "Is, Guc" covers all aspects of working life and aims sharing new developments in industrial relations and human resources also adding values on related disciplines. "Is,Guc" The Journal of Industrial Relations and Human Resources is published Turkish or English language.

TARANDIĞIMIZ INDEXLER

Cabell's
Directories
Since 1978

Sociological
Abstracts
CSA ILLUMINA

asos
akademia
sosyal bilimler indeksi

INDEX COPERNICUS
INTERNATIONAL

INDEX
ISLAMICUS

Dergide yayınlanan yazılardaki görüşler ve bu konudaki sorumluluk yazarlarına aittir.
Yayınlanan eserlerde yer alan tüm içerik kaynak gösterilmeden kullanılamaz.

All the opinions written in articles are under responsibilities of the authors.
The published contents in the articles cannot be used without being cited

İÇİNDEKİLER

Yıl: **2020** / Cilt: **22** Sayı: **1**

SIRA	MAKALE BAŞLIĞI	SAYFA NUMARALARI
1	**Doç. Dr. Kurtuluş KAYMAZ** **“The Analysis of the Relations Among Normative Beliefs, Self-Efficacy and Intention to Comply within the Frame of Information Security Policies”**	5
2	**Dr. Öğr. Üyesi Evrim GÜLERYÜZ, Dr. Deniz GİRAY** **“İstismarcı Yönetim Ölçeğinin Geçerlik ve Güvenirlik Çalışması”**	25
3	**Dr. Öğr. Üyesi Erdem BAĞCI, Öğr. Gör. Duygu ÇELİK** **“Dış Ticaret Dengesi İle Ekonomik Büyüme Arasındaki İlişki: Türkiye’de Ekonometrik Bir Analiz”**	41
4	**Arş. Gör. Elif Nur ALPER** **“Evden İşyerine Ulaşımda Yolda Geçen Zamanın Çalışma Yaşamının Kalitesine Etkisi”**	57
5	**Dr. Öğr. Üyesi Pelin ŞAHİN YARBAĞ** **“Finans Sektörü Çalışanlarının İş Tatminleri İle İK Yönetimi Modellerinin İlişkisi”**	75
6	**Dr. Çağrı KADEROĞLU BULUT** **“Gazetecilerin Gündelik Hayat Deneyimleri: Sınırlılıklar, İmkanlar, İtirazlar”**	91
7	**Dr. Öğr. Üyesi Mehmet GÜLER** **“Nedenleri ve Sonuçları Bakımından Mobbing”**	117

THE ANALYSIS OF THE RELATIONS AMONG NORMATIVE BELIEFS, SELF-EFFICACY AND INTENTION TO COMPLY WITHIN THE FRAME OF INFORMATION SECURITY POLICIES

Kurtuluş KAYMAZ[1]
Uludağ University
Faculty of Economics and Administrative Sciences
Department of Business Administration
Görükle Campus, Bursa, Turkey
kurtuluskaymaz@uludag.edu.tr

ÖZET

Bilgi ve iletişim teknolojilerinin yoğun kullanımı, bilgi güvenliğinin sağlanması bir gereklilik haline gelmiştir. Siber platformlara yapılan saldırılar ve bilgi kaybı olasılığı kurumları bilgi güvenliği süreçlerine yatırım yapmaya zorlar. Bilgi güvenliği kavramı, teknolojiye dayalı önlemleri çok daha fazla gerektiriyor gibi görünse de, insanın bu süreçteki rolü zamanla daha önemli hale gelmiştir. Kurumsal bir bakış açısından bakıldığında, çoğu durumda enformasyon riskine yol açan vakalarda insan kaynaklı hatalar olduğu görülmektedir. Bu nedenle, insan faktörünü bilgi güvenliği politikalarına uygun davranmaya zorlayan yöntemler geliştirilmeye çalışılmıştır. Normatif inançlar ve öz-yeterlik, verilen uyum sürecinde bilgi güvenliği politikalarıyla ilgili iki önemli değişken olarak ön plana çıkmaktadır. Bu nedenle, bu çalışma normatif inançların ve öz-yeterlik değişkenlerinin bilgi güvenliği politikalarına uyum sağlamaya çalışan birey üzerindeki etkilerini incelemeyi amaçlamaktadır. Araştırma Ar-Ge merkezlerine sahip kurumlarda yürütülmüştür. Araştırma sonucunda iki ana bulguya ulaşılmıştır. İlk bulgu, normatif inançların bilgi güvenliği politikalarına uyma niyeti üzerinde olumlu bir etkiye sahip olduğudur. İkinci bulgu ise, öz-yeterliliğin, bilgi güvenliği politikalarına uyma niyetini de olumlu etkilediğidir.

Anahtar Kelimeler: Bilgi güvenliği, bilgi güvenliği davranışı, normatif inançlar, öz-yeterlilik, uyma davranışı.

[1] Associate Professor.

ABSTRACT

In accordance with the intensive usage of information and communication technologies, maintaining information security has become a necessity. Attacks in cyber platforms and information loss probability force institutions to invest in information security processes. Although the concept of information security seems to require technology based precautions more often than not, the role of human in this process has become more critic in time. When considered from an institutional point of view, it is seen that there are human-based errors in most of the cases that resulted in information loss. Therefore, it has been pursued to develop methods that force human factor to behave in compliance with information security policies. Normative beliefs and self-efficacy become prominent as two important variables related to information security policies in the given compliance process. Thus, the present study aims to examine the effects of normative beliefs and self-efficacy variables on the individual who is trying to adapt to information security policies. The research has been conducted in institutions with R&D centers. The research has reached two main findings. The first finding is that normative beliefs have a positive effect on intention to comply with information security policies. The second finding is that self-efficacy also positively affects the intention to comply with information security policies.

Keywords: Information security, information security behavior, normative beliefs, self-efficacy, intention to comply.

INTRODUCTION

Information security risks have been threatening working and social life increasingly. According to World Economic Forum 2016 Report, cyber-attacks are defined as a technological risk in the Global Risk list. Data theft is ranked as 8th in the 10 Most Important Global Risks list in the same report. According to MMC Cyber Handbook (2018) data, 1.1 billion users were attacked in 2016 due to cyber vulnerability. In the last 8 years, cyber-attacks has reached to 7.1 billion users. In the report mentioned above, it is also indicated that from the point of malicious software for ransom an average of 1.077 $ ransom was obtained from 463.841 cyber-attacks in 2016. It is underlined that cyber-attacks have concentrated particularly on energy, health, wholesale and retail sale, finance and production industries. In a different report (The Global State of Information Security Survey-2018), it is stated that 38% of the cyber-attacks experienced in Singapore in 2017 resulted from the errors of the existing personnel. In Data Breach Investigations Report (2017), it is underlined that the personnel are often in-house collaborators who are rationally used in outer attacks and that they participated in such attacks in order to earn money and therefore their access to information which do not directly related to their work should be limited and that it would be useful if they were kept under observation. In another report (Klahr et al., 2017), it is signified that cyber-attacks are not always external and that the errors made by the personnel, use of non-current programs, use of unreliable anti-virus programs or lack of knowledge and lack of awareness of the personnel about cyber security have all create serious gaps.

While information security policies are developed in organizations, the issue of how the personnel should act within the frame of the given policies is often neglected. The concept of information security is usually interpreted with a technological point of view and user perspective becomes of secondary importance. More often, technology based solutions (firewalls, anti-virus softwares and VPNs) are not able to produce satisfactory solutions for eliminating security problems. Information technologies define "human" as the most critical variable in terms of resisting cyber-attacks. Therefore, administrative and behavioral precautions that will enable the personnel to act in accordance with information security policies gain vital importance (Kirsch and Boss, 2007). It is seen that adaptation to information security policies has been accelerated particularly with practices such as raising the awareness of the individuals and providing training for individuals (Kim et al., 2014). Personnel oriented errors cause deeper and more serious information security gaps than technical errors (Ahmed et al., 2012; Pollock, 2017). Ahmed et al. (2012), divide personnel oriented errors into 3 categories. i) errors caused by personnel's lack of skill, ii) errors caused by not acting in accordance with the rules formed within the scope of information security policies and iii) errors caused by personnel's lack of knowledge. Lewis (2003) points out that 65% of the information security gaps that result in economic loss are caused by human factor.

The present study aims to display relative effect of normative beliefs and self-efficacy in developing personnel's behavior compatible with information security policies by emphasizing "human-oriented" errors. In information security literature, there are a limited number of individual oriented studies. Within the context of planned behavior model, the behavior model developed by Bulgurcu et al. (2010) that focuses on awareness raising, attitude development and generating intention to comply within the frame of information security policies is the most cited study in the related literature. In the aforementioned behavior model, it is indicated that information security tendency takes shape under the effect of normative beliefs and self-efficacy variables. In normative beliefs, studies by (Karahanna and Straup, 1999; Kim et al. 2014; Herath and Rao, 2009; Lee et al., 2016; Li, 2015) and in self-efficacy, studies by (Bandura, 1977; Woon et al., 2005; Workman, 2008; Rhee et al., 2019) are the prominent ones in information security literature.

The model shown in Figure 2 is taken as a basis for the present study. Following primary literature review, the hypotheses to be tested within the frame of the model have been formed. Obtained results have been discussed comparatively with similar studies in related literature. The study is completed with the statements regarding the limitations and scope of further studies.

Theoretical Framework

Theory of Planned Behavior

Theory of planned behavior related to this study become prominent in information security literature. "*Theory of reasoned action*" (Ajzen and Fishbein, 1980) perspective has been extended by Ajzen and Madden (1996) and "perceived behavior control" variable is added to the new version. "Intention-compliance tendency" is the major factor in the new model enables orientation towards a behavior. In this context intention indicates how willing an individual is to exhibit a behavior and how much effort the individual plans to exert. The power of intention (compliance tendency) towards a behavior is, in a sense, the indicator of the performance that will be displayed. Planned behavior theory states that there are three variables that create intention to comply. These are; behavior oriented attitude, normative beliefs (subjective norms) and self-efficacy (perceived behavior control) (Ajzen, 1991). Within the scope of planned behavior theory, the present study focuses on normative beliefs and self-efficacy variables that are supposed as effective on intention to comply in information security behavior.

Protection Motivation Theory

When Rogers (1975) developed the first protection motivation theory that defines how an individual should behave when faced with a threat; the researcher indicated that this is a cognitive appraisal process and that there are three cognitive factors that dominate the behavior of individuals when in fear. These are i) threat severity, ii) threat vulnerability iii) response efficacy. Expanding the previous model in 1983, Rogers addressed the importance of information resources as well and referring to Bandura's (1977) social cognitive theory added "self-efficacy" variable to the model. Protection motivation theory is basically built on two main foundations. These are appraisal of the threat and coping with the threat (Figure 1a). Self-efficacy is indicated as an important variable included in the model as a response to the threat. When the model related with protection motivation theory is interpreted within the scope of information security policies, it is assumed that individual appraises first the threat then how to deal with this threat against any internal and/or external attack that threatens information security system.

While appraising this cognitive process, the individual uses the information resources and prior experiences and develops a method to deal with the threat. At a more specific level, while resisting against information security threat, the individual uses self-efficacy and creates a protection zone by considering the response costs. The overall model of protection motivation theory and self-efficacy variable in this process is shown in Figure 1a and Figure 1b (Floyd et al., 2000)

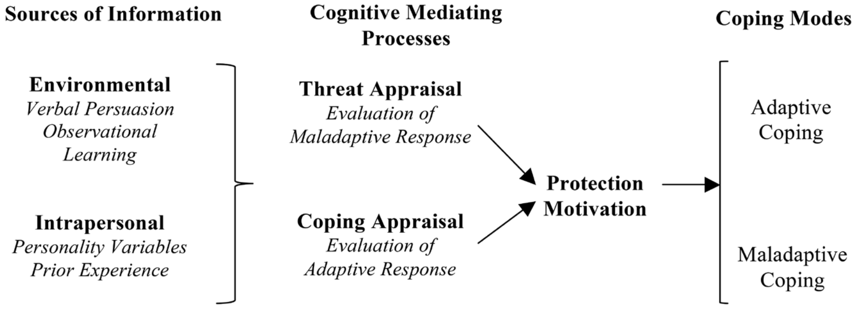

Figure 1a: Overall Model of Protection Motivation Theory

Resource: Floyd, D.L., Prentice-Dunn, S., and Rogers, R.W. (2000). "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology*, 30(2), 407-429.

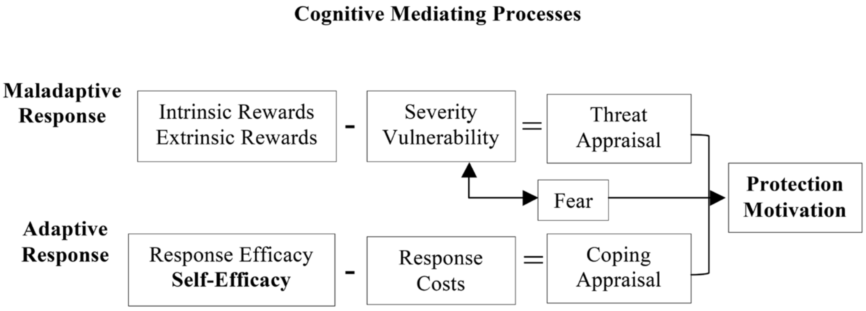

Figure 1b: Cognitive Mediating Processes

Resource: Floyd, D.L., Prentice-Dunn, S., and Rogers, R.W. (2000). "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology*, 30(2), 407-429.

Normative Beliefs and Self-Efficacy in Intention to Comply with the Information Security Policies

In the study by Bulgurcu et al. (2010), the general framework of information security behavior and antecedents of information security policy compliance are defined. Accordingly, information security awareness, benefits of compliance, costs of compliance and noncompliance are indicated as initial factors to develop an information security attitude. On the other side, it is stated that attitude, normative beliefs and self-efficacy affects intention to comply with information security policies (Kim et al., 2014). The present study focuses only on normative beliefs and self-efficacy factors that are stated to be effective on intention to comply.

Normative beliefs refer to the "perceived social pressure" from executives and peers who are considered as a reference point in compliance to the requirements of information security policies (Puhakainen, 2006). Normative beliefs characterize social pressure corresponds to the question "What would other people think about this task that I am going to do?" (Erten, 2002). It is seen that normative beliefs are a driving force in terms of increasing the intention for information security practices (Karahanna and Straup, 1999). As part of information security practices, it is claimed that if individual believe that their executives, IT department or other colleagues expect them to comply with information security policies, they tend to further participate to security actions (Herath and Rao, 2009). As it is seen, social pressure for compliance may stem from colleagues as well as executives. In their study Bulgurcu et al. (2002) point out that within the scope of planned behavior theory (Ajzen, 1991) normative beliefs are one of the factors that trigger compliance to information security policies. In another study (Pahnila et al., 2007) it is indicated that as a member of the social structure, the individual's interaction with others has an effect on their own behaviors. In this context, it is assumed that individuals who are believed to be influential in an environment play distinct roles in the occurrence of a specific behavior or not. Regarding compliance to information security policies, Lee et al. (2016) expressed the fact that when executives and colleagues have a positive attitude towards complying to information security rules this will effect individuals' compliance tendency to information security policies. Li (2015) emphasizes that normative belief factor does not lead home computer users to a behavior towards providing information security and indicates that normative beliefs variable is a factor that affect compliance to information security policies only in organizational structures. In summary, normative beliefs are an intrinsic motivation factor provides compliance to the rules and principles of information security (Siponen, 2000).

In information security literature, it is indicated that self-efficacy is another variable that generates tendency to comply to information security policies (Bulgurcu et al., 2010; Woon et al., 2005; Maddux and Rogers, 1983). In social cognitive theory context, self-efficacy is the provision of the individual on how successful they will be in overcoming the difficulties they may face in the future (Bandura, 1977). From another point of view, it is the belief of the individual about his/her own skills in order to implement a certain behavior. It is stated that the skills support coping behavior of the individual and have a positive relationship with behavioral change (Bandura et al., 1980). In computer use context self-efficacy (Davis et al., 1989; Pahlina et al., 2007) is defined as the assessment of an individual's skills about using a computer and it is stated that self-efficacy is an important indicator of user behavior (Woon et al., 2005). As for compliance to information security policies, self-efficacy (Kim et al., 2014; Li, 2015) is used to express the situation where individual evaluates whether they have adequate knowledge, skills and techniques regarding information security process. Floyd et al. (2002) define self-efficacy as the skills acquired to cope with information security breaches.

Within this context, self-efficacy indicators such as data back-up, updating virus programs, creating and updating passwords, knowing how to react technically to a possible security breach, knowing how to act in the case of data loss, mastery of the software necessary within the scope of information security practices, knowing information security procedures etc. have importance in coping with information security breaches. It is remarked that individuals with high self-efficacy show more effort to accomplish a task, are more insistent and not afraid to try again when compared to the ones with low self-efficacy (Bandura, 1977). In this regard, Workman et al. (2008) stated that individuals with high self-efficacy tend to use technology more effectively and may be more efficient in learning how to apply information security practices. In the same study, it is expressed that individuals with high self- efficacy have a higher level of awareness regarding information security threats and a better understanding of the coping processes. Another study (Rhee et al., 2009) has found that in the context of information security, self-efficacy is a significant explanatory variable for providing information security. In the same study, it is indicated that self-efficacy also makes positive contributions to the sustainability of the efforts of the personnel to provide information security. At the same time, self-efficacy employs the fundamental skills to deal with stress elements caused by information security (work load, invasion of privacy, etc.) (Ayyagari et al., 2011). Contrary to the studies that emphasize the relationship between self-efficacy and intention to comply with information security policies, Kim et al. (2014), have found that self-efficacy is not an effective variable in compliance to information security policies.

Research Model and Hypotheses

The present study is based on the model displayed in Figure 2 in order to investigate the interaction among normative beliefs, self-efficacy and intention to comply from the point of information security behavior in planned behavior model context. The model focuses on two main effects. The first one is the effect of normative beliefs on intention to comply with information security policies. The second is the effect of self-efficacy on intention to comply with information security policies. In this context, research model and hypotheses are given below.

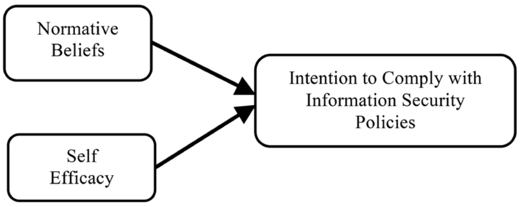

Figure 2: Research Model

H1: In information security behavior, normative beliefs have a positive effect on intention to comply with information security policies.

H2: In information security behavior, self-efficacy has a positive effect on intention to comply with information security policies.

Method, Sample and Scales

Data is collected by using a face to face survey. A pilot study consisting of 50 questionnaires is conducted to test the clarity of the statements and to make pre-validity and reliability analyses. As a result of pilot study, it is seen that statements in the survey are generally understood and no change is needed for items.

The mass of the present research consist of production organizations with R&D or Design Center in Bursa that are established in accordance with The Law numbered 5746 Regarding "The Support of Research, Development and Design Activities". The rationale behind choosing these organizations is that there is intensive brand, patent, industrial design and utility model development in these establishments and requires an advanced information security system. In this context, there are more than 100 businesses with a R&D or Design Center in Bursa. However, it is not possible to reach such a large group due to time and financial costs. Therefore, data is gathered from a certain sample group. Sample group is generated according to "snowball sampling" technique. The businesses with ISO 27001 information security certificate and ones that developed processes that are compatible with information security policies and the ones where more attention is paid to information security are preferred for the study. In this scope, the questionnaire is given to a total of 215 participants from automotive, textile, glass and cable industries.

Five point Likert Scale [Strongly Disagree (1)- Strongly Agree (5)] is used in the study. The scales used in the study and their statistical data are given below.

Normative Beliefs Scale

Normative belief scale is generated by using 8 items from Herath and Rao's (2009) study. 6 items which are considered as compatible to the aim of the present study are included in the questionnaire. In the original study cronbach alpha value is 0.90. In the present study cronbach alpha coefficient of normative beliefs scale is 0.87.

Self-Efficacy Scale

Two studies are used for self-efficacy scale. The first one is conducted by Lee et al. in 2016. In the study by Lee, 7 items is used to measure self-efficacy level. In the original study, cronbach alpha value of these 7 items is 0.90 and all 7 of these items are included in the present study. The second study used for self-efficacy scale is carried out by Rhee et al. in 2009. In their study Rhee et al. used 11 items for self-efficacy variable. 4 statements that are compatible with the aim of the present study included in the research. Cronbach alpha value of 11 items used in the original study is 0.97. Cronbach alpha coefficient of 11 items that are generated from two resources used in this study is 0.88.

Intention to Comply Scale

The study by Ajzen (1991) and Bulgurcu et al. (2010) are taken as a basis for intention to comply. In Ajzen's study, a set of 3 items is used to find out individual's intention to behave and Bulgurcu et al. are used these 3 items for defining comply to information security policies. In the present study, these 3 items are included and cronbach alpha value is 0.71.

Items and sources used in this study are given in Table 1.

Table 1: Variables, Items and Sources Related with Variables of the Model

Variable	Items	Source
Normative Beliefs	1. Top management thinks I should follow organizational IS security policies. 2. My boss thinks that I should follow organizational IS security policies. 3. My colleagues think that I should follow organizational IS security policies. 4. The information security department in my organization thinks that I should follow organizational IS security policies. 5. Computer technical specialists in the organization think that I should follow organizational security policies.	Herath and Rao (2009)
Self-Efficacy	1. I can install an information security application. 2. I can back up data for information security. 3. I know how to respond when hacking or malware occurs. 4. I know the response procedures when an information security accident occurs. 5. I know the chief information security officer (CISO) in my organization. 6. I know the reporting procedure for losses from information security failure. 7. I know the legal liability for information security violation. 8. I feel confident handling virus infected files. 9. I feel confident understanding terms/words relating to information security. 10. I feel confident getting help for problems related to my information security. 11. I feel confident updating security patches to the operating system.	Lee et al. (2016) Rhee et al. (2009)
Intention to Comply	1. I intend to comply with the requirements of the ISP of my organization in the future. 2. I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future. 3. I will learn more about how to strengthen my information security.	Ajzen (1991) Bulgurcu et al. (2010)

Findings

Demographic Profile of the Participants

4 items (gender, age, education and length of service) used to determine demographic characteristics of the participants as displayed in Table 2.

Table 2: Demographic Characteristics

		N	%
Gender	*Female*	81	37.7
	Male	134	67.3
Age	*Up to 20*	-	-
	21-30	68	31.6
	31-40	97	45.1
	41-50	39	18.1
	51 and over	11	5.1
Education	*Primary School*	-	-
	High School	8	3.7
	Associate's Degree	5	2.3
	Bachelor's Degree	160	74.4
	Master's Degree	39	18.1
	PhD Degree	3	1.4
Length of Service	*Less than 1 year*	27	12.6
	1-5 years	74	34.4
	6-10 years	44	20.5
	11-15 years	24	11.2
	16 years and over	46	21.4

Correlation Analysis

Positive relations are found among the variables in the present study (Table 3). In this regard, the most significant linear relationship is between normative beliefs and self-efficacy variables (0.470). On the other hand, positive relationships are determined between normative beliefs and intention to comply (0.401) and between self-efficacy and intention to comply (0.299). It is clear that the strongest relation is between normative beliefs and self-efficacy so it can be said that focusing on normative beliefs could develop individual's self-efficacy related to information security practices.

Table 3: Correlation Coefficient, Mean, Standard Deviation and Cronbach Alpha Values among Normative Beliefs, Self-Efficacy and Intention to Comply

	N	Mean	Standard Deviation	Cronbach Alpha	NB	SE	IC
Normative Beliefs (NB)	215	4.08	0.55	0.87	1		
Self-Efficacy (SE)	215	3.57	0.62	0.88	.470**	1	
Intention to Comply (IC)	215	4.19	0.49	0.71	.401**	.299**	1

***. Correlation is significant at 0.01 level (2-tailed).*

Confirmatory Factor Analysis

Confirmatory factor analysis is performed to test whether the consistency of a specified measurement model is statistically significant or not. As a difference from factor analysis being performed by conventional methods, confirmatory factor analysis is used to test the verification of factorial construct determined by the researcher in advance. At this point of view, it is assumed that more than one latent variables thought to be constructed by scale items are explained by another latent variable and consistency of this assumption with the data is tested.

Various goodness of fit indices which have statistical functions in evaluation of model consistency. In the analysis, goodness of fit index-**GFI**, standardized **RMR** and root mean square error of approximation-**RMSEA**, Bentler comparative fit index-**CFI** have been considered. For determining the performance of the model, above mentioned indices are expected to have specified fit values. The values are illustrated in Table 4.

Table 4: Standard Goodness of Fit Indices

Goodness of Fit Measures	Goodness of Fit Values	Acceptable Goodness of Fit Values
RMSEA	0.00<RMSEA<0.05	0.05<RMSEA<0.10
SRMR	0.00<SRMR<0.05	0.05<SRMR<0.10
GFI	0.95<GFI<1.00	0.90<GFI<0.95
CFI	0.95<CFI<1.00	0.90<CFI<0.95

Within the scope of the obtained data, confirmatory factor analysis is conducted in order to test the validity of the measuring tools by using AMOS statistical software. A total of 4 items (1 item from normative beliefs variable, 2 items from self-efficacy variable and 1 item from intention to comply variable) are excluded from the analysis due to their low factor loads. Accordingly, goodness of fit values are determined on the basis of normative beliefs, self-efficacy, intention to comply and whole model. It is seen that (Table 5) goodness of fit values are within the acceptable limits which showed validity of the measuring tools.

Table 5: Research Model Goodness of Fit Values

	χ^2	*df*	χ^2/df	GFI	CFI	RMSEA	SRMR
Normative Beliefs	9,939	7	1,420	0,98	0,99	0,04	0,03
Self-Efficacy	104,412	24	4,350	0,90	0,92	0,12	0,05
Intention to Comply	0,000	0	-	1,00	1,00	0,70	0,00
Whole Model	241,115	96	2,512	0,87	0,93	0,08	0,09

It is indicated that hypothesis of normality is met when skewness and kurtosis values are between -1 and +1 (Kalaycı, 2005). Normality test results in this study show that skewness and kurtosis values of the variables are generally between -1 and +1 [Normative Beliefs (-0,361/0,037); Self-Efficacy (-0,043/ 0,021); Intention to Comply (-0,049 /1,030)).

Structural Equation Modeling Results

When analysis results are reviewed it is determined that %23 [R^2= 0.23] of dependent variable (intention to comply) is explained by the independent variables (normative beliefs and self-efficacy) included in the model. Parameter estimations of the relations between variables are given in Table 6.

Table 6: Parameter Estimations for The Model

		Estimation	S.E	C.R	p value
Intention to Comply Normative Beliefs	←	0,357	0,106	3,355	0,000
Intention to Comply Self-Efficacy	←	0,212	0,050	4,206	0,000

When parameter estimations of the model are examined, it is seen that p value is significant in all relations. Within the scope of the investigation, initially it is determined that normative beliefs have a positive and significant effect on intention to comply within the information security policies (parameter estimation = 0.357; p<0.05). Therefore, "*H1: In information security behavior, normative beliefs have a positive effect on intention to comply with information security policies.*" hypothesis is accepted. Similarly, analysis results show that self-efficacy also has a positive and significant effect on intention to comply within the information security policies (parameter estimation=0.212; p<0.05). From this viewpoint, "*H2: In information security behavior, self-efficacy has a positive effect on intention to comply with information security policies.*" hypothesis is accepted. As for the relative significance level of independent variables on dependent variable, self-efficacy variable (4.206) is more effective on intention to comply than normative beliefs variable (3.355). From this perspective, it is understood that the attempts to increase self-efficacy would create more effective results while generating intention to comply with information security policies. Analysis results of structural equation modeling are given in Figure 3.

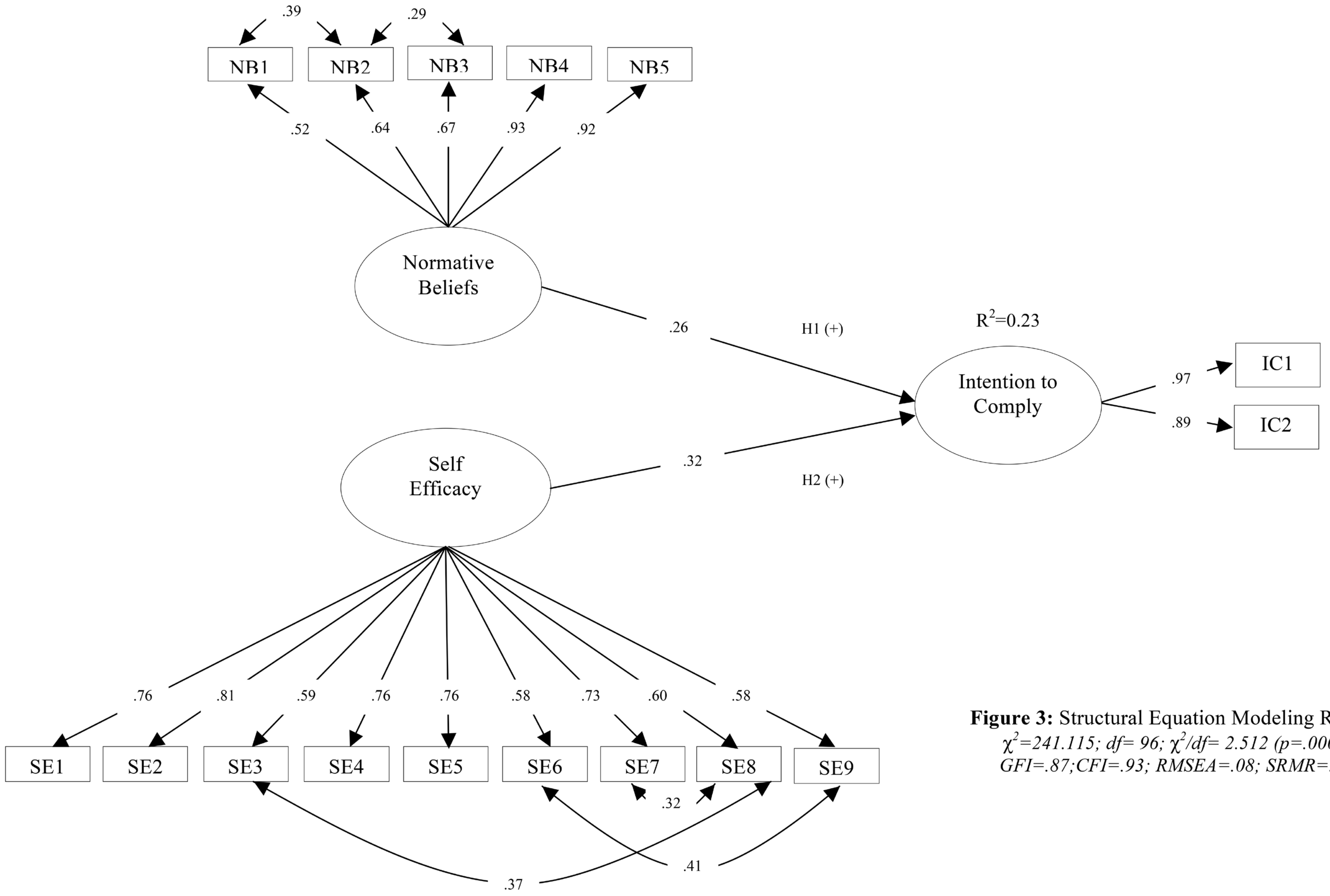

Figure 3: Structural Equation Modeling Results
χ^2=241.115; df= 96; χ^2/df= 2.512 (p=.000);
GFI=.87;CFI=.93; RMSEA=.08; SRMR=.09

Conclusion

Providing information security has critical importance in order to protect information asset in organizations. Developing information security policies, executing the requirements of ISO 27001 Information Security Certification, investigating in information technologies have become strategic priorities of the businesses that generate knowledge and conduct information-based competition. Besides gaining the technical qualification around information security, organizations make an effort for "human" factor to exhibit behaviors that are compatible with information security policies. Human beings constitute the weakest link in information security chain and the factor that causes the hardest challenge in providing security. Low information security awareness of the personnel, their lack of knowledge about the financial losses when security weakness appear, lack of information security skills about the security processes or lack of guidance in accordance with information security policies cause "human oriented" errors and create security information threat for the businesses. Thus, "person-information security fit" has become one of the critical areas in providing information security. Despite that compliance to information security policies may create negative results on a personal basis as well. Work impediments due to bureaucracy created by information security policies, tracking mechanisms that may cause invasion of privacy may increase stress to emerge on the basis of information security. Within this framework, "human" has become the most critical element of information security practices.

The first finding of the study is that within the scope of information security practices, normative beliefs have a positive effect on intention to comply to information security. In other words, it is concluded that social pressures by executives and/or colleagues, employer or director/specialits of information security unit are effective on a person's intention to comply with information security policies. This finding is similar to the study by Bulgurcu et al. (2010) which explains the nature of the relationship between normative beliefs and intention to comply. Similarly, this finding matches with the finding of the study conducted by Lee et al. (2016) which indicates the fact that exhibition of positive attitude by executives and colleagues towards compliance to information security rules is effective on an individual's intention to comply with information security policies. In this context, this first finding shows that the social pressure block (executives, colleagues, employer, information security manager and specialists) is critical for adapting information security policies. The fact that social pressure block orally inculcates in accordance with information security policies, uses a communicative language compatible with the policies in internal communication channels, makes statements at every opportunity about the significance of the information security may produce effective results in individual's intention to comply and exhibition of compliance behavior. When viewed from the point of mean values (on the basis of all items mean values are 4 and above 4), normative pressure sides (employer, executives, colleagues, specialists) in the organization where the present research was conducted have exhibited attitude toward intention to comply with information security policies.

The second finding of the study is that self-efficacy positively affects intention to comply with information security policies. This finding is similar to the results of the related studies in the literature (Bulgurcu et al. 2010; Woon et al., 2005; Workman et al., 2008; Kim et al., 2004). In this regard, the fact that an individual possesses the required competence within the frame of information security practices increases intention to comply. The beliefs of the individual about having the required qualifications which could be specified as mastery of information security software, data back-up, reacting information security threats, knowing personal responsibilities and legal obligations regarding information security, performing program updates supports their intention to comply with information security policies. When mean values related with self-efficacy items are examined, it is seen that personnel of the institution where the research was conducted have shortcomings regarding how they should act in case of an attack or malware (3.50). Besides, it is understood that when there is an information security problem, personnel do not know how they should procedurally act (3.62). Similarly, it is observed that when there is any data loss, personnel do not have adequate level of knowledge about how they should report this issue (3,63); when there is information security violation, they could not grasp what their personal legal obligations are (3,33) and that they do now know how they could save virus-infected files (2.90) and could not handle required update for information security system effectually (3.20). From this point of view, it is determined that there is a need to emphasize the development of information security competence via training programs of the organization.

Another remarkable finding of the present study is that self-efficacy variable has more significant effect on the individual's intention to comply than normative beliefs. In other words, while generating intention to comply to information security policies, attempts to increase self-efficacy of individuals would create more effective results than generating normative pressure within the context of information security practices.

Generally, it can be said that information security practices which are initially thought within the frame of informatics is related to human behavior as well. Effectiveness of information security policies significantly depends on the ability of the personnel to exhibit compliance behavior. There are many information security threats that may appear as result of personal negligence of the human. When it is considered that information security gaps impose a burden on businesses at financial, administrative and social levels, the need for the businesses to manage human-based information security processes becomes important. In this regard, as is underlined in planned behavior theory, it is necessary to re-assess normative beliefs and self-efficacy factors which affect intention to comply.

Limitations and Further Research

The most significant limitation of this study is the fact that the issue of information security contains sensitivity and that businesses tend to approach the research about this issue with caution. Many of the executives have negative approach when information security vulnerability of their company is unfolded and shared. This approach has prevented to increase the number of questionnaires used in the study. Questionnaires, particularly, are fulfilled and obtained via personal connections.

The study conducted by Kaymaz and Erbi (2018) has investigated the relationship among work impediments, stress in information security and invasion of privacy in information security behavior. The present study has examined the other dimensions of information security behavior such as intention to comply, normative beliefs and self-efficacy. As a further research it is projected to conduct a study to investigate "information security awareness" phase of information security behavior.

REFERENCES

Ajzen, I. (1991). "The Theory of Planned Behavior", *Organizational Behavior and Human Decision Processes*, 50, 179-211.

Ajzen, I., Fishbein, M. (1980). Understanding Attitude and Predicting Social Behavior, Englewood Cliffs, NJ: Prentice-Hall.

Ajzen, I., and Madden, T.J. (1986). "Prediction of Goal Directed Behavior: Attitudes, Intentions, and Perceived Behavioral Control", *Journal of Experimental Social Psychology*, 22, 453-474.

Ahmed, M., Sharif, L., Kabir, M. ve Al-Maimani, M. (2012). "Human Errors in Information Security", *International Journal of Advanced Trends in Computer Science and Engineering*, 1(3), 82-87.

Ayyagari, R., Grover, V. ve Purvis, R. (2011). "Technostress: Technological Antecedents and Implications", *MIS Quarterly*, 35(4), 831-858.

Bandura, A. (1977). "Self Efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological Review*, 84, 191-215.

Bandura, A., Adams, N., Hardy, A., and Howells, G. (1980) "Tests of the Generality of Self Efficacy Theory," *Cognitive Therapy and Research*, 4, 39-66.

Bulgurcu, B., Çavuşoğlu, H. ve Benbasat, I. (2010). "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", *MIS Quarterly*, 34(3), 523-548.

Data Breach Investigations Report (2017). "Verizon Enterprise" 10th Edition.

Davis F.D., Bagozzi R.P., Warshaw P.R. (1989). "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models", *Management Science*, 35 (8), 982-1003.

Floyd, D.L., Prentice-Dunn, S., and Rogers, R.W. (2000). "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology*, 30(2), 407-429.

Herath, T. ve Rao, H.R. (2009). "Herath Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness", *Decision Support Systems*, doi: 10.1016/j.dss.2009.02.005

Kaymaz, K. ve Erbi, H. (2018). "Bilgi Güvenliğinde Stres Faktörlerinin İş Tatmini Üzerindeki Etkileri: Ar-Ge Merkezi Olan İşletmeler Üzerinde Bir Araştırma", *"İş, Güç" Endüstri İlişkileri ve İnsan Kaynakları Dergisi*, 20(4), 91-112.

Kalaycı, Ş. (2005). SPSS Uygulamalı Çok Değişkenli İstatistik Teknikleri, Ankara: Asil Yayın Dağıtım.

Karahanna, E. and Straub, D.W. (1999). "The Psychological Origins of Perceived Usefulness and Ease-of-Use", *Information & Management,* 35, 237-250.

Klahr, R., Shah, J.N., Sheriffs, P., Rossington, T., Pestell, G., Button, M. ve Wang, V. (2017). "Cyber Security Breaches Survey, Main Report".

Kim, S.H., Yang, K.H. ve Park, S. (2014). "An Integrative Behavioral Model of Information Security Policy Compliance", *Scientific World Journal*, ID 463870, 1-12.

Kirsch, L. ve Boss, S. (2007). "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines", International Conference on Information Systems Proceedings. 103.

Lee, C., Lee, C.C. ve Kim, S. (2016). "Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity", *Computers and Security*, 59, 60-70.

Lewis, J. (2003). "Cyber Terror: Missing in Action", *Knowledge, Technology & Policy*, 16(2), 34-41.

Li, Y. (2015). "Users' Information Systems (IS) Security Behavior in Different Contexts", University of Oulu, Finland, ISBN 978-952-62-0938-8.

Maddux, J.E. ve Rogers, R.W. (1983) "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change", *Journal of Experimental Social Psychology*, 19, 469-479.

MMC Cyber Handbook (2018). "Perspectives on the Next Wave of Cyber", Marsch and McLennan Global Risk Center.

Pahnila, S., Siponen, M. and Mahmood, A. (2007). "Employees' Behavior Towards IS Security Policy Compliance", Proceedings of the 40th Hawaii International Conference on System Sciences, 1-10.

Pollock, T. (2017). "Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS)", Kennesaw State University Proceedings on Cybersecurity Education, Research and Practice 2.

Puhakainen, P. (2006). A Design Theory for Information Security Awareness, Faculty of Science, Department of Information Processing Science, University of Oulu, ISBN 951-42-8114-4.

Rhee, H.S., Kim, C. ve Ryu, Y.U. (2009). "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior", *Computers & Security*, doi:10.1016/j.cose.2009.05.008

Rogers, R.W. (1975). "A Protection Motivation Theory of Fear Appeals and Attitude Change", *Journal of Psychology*, 91, 93-114.

Rogers, R.W. (1983). "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation", In J. Cacioppo & R. Petty (Eds.), Social Psychophysiology. New York: Guilford Press.

Siponen, M.T. (2000). "A Conceptual Foundation for Organizational Information Security Awareness", *Information Management & Computer Security*, 8(1), 31-41.

The Global State of Information Security Survey, PWC, January 2018

Woon, I. M. Y., Tan, G. W. and Low, R. T. (2005). "A Protection Motivation Theory Approach to Home Wireless Security", Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas, 367-380.

Workman, M., Bommer, W.H. and Straub, D. (2008). "Security Lapses and The Omission of Information Security Measures: A Threat Control Model and Empirical Test", *Computers in Human Behavior*, 24, 2799-2816.

World Economic Forum (2016). "The Global Risks Report", 11.Baskı