BİLGİ GÜVENLİK FARKINDALIĞINI ETKİLEYEN FAKTÖRLERİN BELİRLENMESİ: YÜKSEKOKUL ÖĞRENCİLERİ ÜZERİNE BİR İNCELEME

Ömer Faruk RENÇBER [*] Sinan METE [**]

Geliş Tarihi (Received): 29.02.2016 – Kabul Tarihi (Accepted): 06.12.2016

ÖZ

Bu çalışmada yüksekokul öğrencilerinin bilgi güvenlik farkındalığı davranışlarını etkileyen faktörler ve bu faktörlerin etki düzeyleri incelenmiştir. Bilgi güvenlik farkındalığı davranışlarını ölçebilmek için Parsons vd. (2013) tarafından geliştirilen HAIS-Q (İnsan Yönelimli Bilgi Güvenlik Farkındalığı Anketi) ölçeği kullanılmıştır. Çukurova Üniversitesi Kozan MYO kapsamında, bölümler arası kotalı örnekleme yöntemiyle seçilen 420 öğrenciye anket uygulaması yapılmış ve elde edilen veriler öncelikle keşfedici faktör analizi ve ardından yapısal eşitlik modeli teknikleri ile analiz edilmiştir. Çalışmanın sonucunda bilgi güvenlik farkındalığını en çok etkileyen faktörlerin şifre yönetimi, mobil internet kullanımı, e posta ve internet kullanımı ve sosyal ağ sitelerinin kullanım davranışları olduğu sonucuna ulaşılmıştır.

Anahtar Kelimeler: *Bilgi Güvenlik Farkındalığı, Yapısal Eşitlik Modellemesi, Bilgi Güvenliği*

[*] Öğr. Gör. Çukurova Üniversitesi, Kozan Meslek Yüksek Okulu, ofrencber@cu.edu.tr
** Yrd. Doç. Dr. Aksaray Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü, sinanmete@hotmail.com

DETERMINING THE FACTORS AFFECTING THE KNOWLEDGE SECURITY AWARENESS: A RESEARCH ON VOCATIONAL STUDENT

ABSTRACT

In this study, the factors affecting the information security awareness behaviors of college students and the effect levels of these factors were examined. In order to measure the knowledge security awareness behavior was used Parsons et al (2013) developed by HAIS-Q (Human Aspects of Information Security Questionnaire) scale. Within the scope of Çukurova University Kozan Vocational School, 420 student questionnaires were selected by means of cross-sectional sampling method and the obtained data were analyzed primarily by exploratory factor analysis followed by structural equality modeling techniques. As a result of this study, the most important factors affecting information security awareness are password management, mobile internet usage, e-mail and internet usage and usage behavior of social network sites.

Keywords: *Knowledge Security Awareness, Structural Equation Modelling, Knowledge Security*

GİRİŞ

Kısa sürede yaygınlaşan ve halen yaygınlaşmaya devam eden bilişim teknolojileri, gün geçtikçe hayatımızın vazgeçilmez bir parçası halini almaktadır. Telefon, bilgisayar, tablet gibi cihazlar toplumun sosyal, ekonomik ve diğer alanlarında önemli bir yer tutmaktadır. Günümüzde haberleşme, iletişim ve diğer amaçlarla kullanılan bu cihazların ortak noktasının, hepsinde bulunan internet sistemi olduğu söylenebilir.

1960'lı yıllarda keşfedilen internet teknolojisi; ülkeleri, bölgeleri ve insanları birbirine bağlayan büyük bir araç olarak görülmekte ve dünya çapında birçok alanda çeşitli amaçlarla kullanılmaktadır. Özellikle bilgilerin ve belgelerin aktarılmasında, sosyal arkadaşlık kurma ve mesajlaşmalarda, resim, video gibi paylaşımlarda ve banka hesaplarının yönetilmesi gibi özel işlerde kullanılması internetin önemini artırmaktadır. Bu durum insanın hayatındaki kaynağı veya imkânı doğru kullanması problemini de beraberinde getirmektedir.

Bilgisayar ve diğer teknolojik cihazlardaki bilgi güvenliğini tehdit eden unsurlar, bilişim tehditleri ve kişiye bağlı tehditler olmak üzere iki kısımda incelenebilir. Bilişim tehditleri; internet yoluyla yayılan virüs, kötü niyetli kodlar, erişime açık alanlardaki bağlantılar, hacker saldırıları; kişiye bağlı tehditler ise zayıf şifre yönetimi, açık unutulan e-posta ve diğer kişisel hesaplar olarak örneklendirilebilir.

Pfleeger'e göre (1997:12) bilgi güvenliği kavramı; bilgiye sürekli erişimin sağlanması, bilginin göndericiden alıcısına kadar gizlilik içerisinde, bozulmadan ve başkaları tarafından ele geçirilmeden bütün olarak güvenli bir şekilde iletilmesi olarak tanımlanmaktadır.

Tekerek'e göre (2008:132-138) bilgi güvenliği ilkeleri; gizlilik, bütünlük, erişilebilirlik, log tutma, kimlik tespiti, güvenirlik ve inkâr edememedir. Bunlardan gizlilik, bilginin üçüncü şahısların eline geçmesinin engellenmesini; bütünlük, bilginin göndericiden alıcıya tam olarak ulaşmasını; erişilebilirlik, bilgiye zamanında erişimin sağlanmasını; log (kayıt) tutma, bilgisayarda gerçekleştirilen bütün olayların kayıt altına alınmasını ifade etmektedir. Kimlik tespiti, doğru kişi ile olayı gerçekleştirdiğinden emin olmak; güvenirlik, bilgisayar sisteminden beklenen davranış ile gerçekleşen davranış arasındaki fark ve inkâr edememe ise gerçekleşen olayın veya tutulan kaydın karşı tarafça inkâr edilememesi olarak tanımlanmaktadır.

Günümüzde işletmelerde bilgi güvenliği sağlamak için çeşitli bilişim tekniğine dayanan önlemler alınmaktadır. Ancak bilgi güvenliği için en önemli faktörün personellerin veya kişilerin bilgi güvenlik farkındalığını sağlamak olduğu ifade edilebilir. Bilgi güvenlik farkındalığını sağlamak için ise kurumların sahip oldukları insan kaynaklarını eğitmeleri veya bu konuda bilinçli kişileri istihdam

etmeleri gerekmektedir. Bu açıdan bakıldığında, yüksekokullardaki öğrencilerin bilgi güvenlik farkındalıklarının durum tespiti ve eğitimi büyük önem arz etmektedir.

TÜİK 2014 yılı verilerine göre, Türkiye'de toplam 2 milyon kişi herhangi bir fakülte veya yüksekokula yeni kayıt yaptırmışlardır. Bunların yaklaşık olarak %32'si ön lisans programlarına yerleşmişlerdir. 2013-2014 akademik yılında bütün öğrencilerin %28'i ön lisans programlarına kayıtlı olup bunlardın da %50'si erkek, %50'si bayandır. 2015 yılı itibariyle Türkiye'nin toplam nüfusunun 77 milyon civarı olduğu düşünüldüğünde %10'luk kısmı üniversite öğrencileridir(TÜİK, 2015). Bu oran ülkenin vatandaşlarına ait kişisel bilgi güvenliği politikalarını geliştirmede oldukça önemli bir yer tutmaktadır. Bununla beraber toplam nüfusun %30 civarının 18 yaş altında oldukları dikkate alınırsa mevcut ve gelecekteki yükseköğretim öğrencilerin bilgi güvenlik farkındalığına yaklaşımlarını belirlemek ve bu konuda gerekli önlemleri almak ülke için zorunlu bir hal almaktadır.

Çalışmada öğrencilerin bilgi güvenlik farkındalıkların değerlendirilmesi, farkındalık oluşturmada etkili olan faktörlerin ve bunların etki düzeylerinin belirlenmesi amaçlanmaktadır. Bu amaçla dört bölümden oluşan çalışmanın birinci ve ikinci bölümünde literatür özeti ve yapısal eşitlik modellemesi tanıtılmıştır. Çalışmanın üçüncü kısmında yüksekokul öğrencilerine yönelik uygulanan anketlerle elde edilen veri setine sırasıyla güvenilirlik analizi, keşfedici faktör analizi ve yapısal eşitlik modeli uygulanmıştır. Çalışmanın son bölümünde ise elde edilen bulgular tartışılmıştır.

I. LİTERATÜR TARAMASI

Literatürde bilgi güvenliği yönetimi, bilgi güvenlik farkındalığı konusunda çalışmaların genellikle işletmelerdeki çalışanlar ve yöneticiler üzerine yapıldığı göze çarpmaktadır. Çoğu çalışmada, bilgi güvenlik farkındalığı sağlamak için çalışanların bilişsel ve kültürel yapılarına olumlu katkı sağlayıcı eğitimler ve uygulamalar yapılmasının önerildiği görülmektedir. Aynı zamanda çoğunlukla konuyu bir talimatname kapsamında değil de aynı zamanda çalışanların içgüdüsü, motivasyonu ve kurum içi davranış şekilleri ile ele almak gerektiği savunulmaktadır.

Kruger ve Kearney (2006:289-296), bilgi güvenlik farkındalığını değerlendirme amacıyla bir prototip geliştirmişlerdir. Çalışmalarında altı bölgeyi kanunlara bağlılık, şifreleri gizli tutma, e posta ve internet kullanımı, mobil ekipman kullanımı, güvenlik sıkıntılarını raporlama ve en son gösterilen davranış kapsamında değerlendirmişlerdir. Buna göre, bilgi güvenlik farkındalığı yüksek, orta ve düşük olan bölgeler belirlenmiş ve bulguları tartışmışlardır.

Kegel ve Wieringa (2015:51-56) çalışmalarında kişisel bilişim teknolojilerini yönetmede davranış değişikliklerini incelemiş ve sonuç olarak çalışanların davranışları ve bilgi güvenliklerini esas alan özel bir yazılım geliştirmişlerdir.

Yang vd. (2013:482-490) bilgi güvenlik risk değerlendirmesi problemine VIKOR, Analitik Ağ Süreci (ANP) ve DEMATEL yöntemleri ile çözüm aramışlardır. Saleh vd. (2011:107-118) bilgi güvenlik yönetimini strateji, teknoloji, organizasyon, insan ve çevre faktörlerine göre incelemişlerdir. Shamala vd. (2013:45-52) bilgi güvenlik risk değerlendirme (ISRA) problemine alternatif bir kavramsal çerçeve üretmişlerdir.

Parsons vd. (2013:1-11), organizasyonlarda bilgi güvenlik farkındalığı konusunda çalışanların durum tespitini belirlemek amacıyla bir ölçek geliştirmişlerdir. Ölçek; şifre yönetimi, e posta kullanımı, internet kullanımı, sosyal ağ kullanımı, hata raporlama, mobil bilgisayar kullanımı ve bilgileri elden geçirme faktörlerinden oluşmaktadır.

Siponen (2014:217-224), örgütlerde bilgi güvenlik farkındalığının genellikle çok yüzeysel incelendiğini, insan davranışı ve içgüdüsel motivasyon faktörlerinin göz ardı edildiğini ifade etmiştir. Tsohou vd. (2015) bilgi güvenlik farkındalığının sadece davranışla ilgili olmadığını aynı zamanda bu durumun bilişsel ve kültürel olabileceğini savunmuşlardır. İnsanları davranış ve kültürlerine göre kaderci, çıkarcı, eşitlikçi ve hiyerarşik düzenci olmak üzere 4 kısma ayırmışlar ve insanların bilgi güvenliğinde ne tür davranış gösterdiklerini tespit etmişlerdir. Ayrıca çalışmanın sonunda bu konu ile alakalı önerilerde bulunmuşlardır.

Tekerek vd. (2013), öğrencilerin bilgi güvenlik farkındalığındaki etik anlayışları ile teknolojik anlamda yeterlilikleri arasındaki etkileşim olup olmadığını incelemişlerdir. Bu amaçla geliştirdikleri ölçeğin analiz edilmesi sonucunda, öğrencilerin bilgi güvenlik sorunsalında etik açısından bilinçli oldukları ancak teknoloji açısından yetersiz kaldıklarını tespit etmişlerdir.

Güler vd. (2015), tıp fakültesi öğrencilerinin ve hekimlerin internet ve sosyal ağ kullanımlarını incelemişler ve internet kullanımını tanımlayacak sorular içeren anket uygulaması yapmışlardır. Çalışmada hekimlerin ve öğrencilerin üst düzey bilgi güvenlik farkındalığına sahip olmadıkları hatta büyük bir çoğunluğunun kendilerine ait gerçek bilgileri internet yoluyla bir başkası ile paylaşabilecekleri sonucuna ulaşmışlardır.

Tekerek (2008), bilgi güvenlik problemini yaşayan bir sistem olarak ele almış ve sürecin yönetilebilmesi için bilgi güvenliği yönetim modeli geliştirmiştir. Çalışmada bilgi paylaşım ve aktarımdaki tehditleri; insan kaynaklı tehditler, fiziksel tehditler, yazılım tehditleri, korunmasızlık, eğitim, bilinç ve güvenlik politikaları şeklinde maddelemiştir.

Gökmen ve Akgün (2015), Bilgisayar ve Öğretim Teknolojileri bölümü öğrencileri üzerine yaptıkları araştırmada kişilerin bilgi koruma, yönetme ve güvenirliği sağlama konularındaki yaklaşımlarını incelemişlerdir. Çalışmanın sonucunda bilgi güvenlik farkındalığının cinsiyete, yaşa, bilgisayar sahibi olmasına veya günlük bilgisayar kullanımına bağlı olarak değiştiği ve genel olarak akademik bölümlerde bilgi güvenliği konusunda dersler konulmasının faydalı olabileceği sonucuna ulaşmışlardır.

Hansche (2001), çalışmasında bilgi güvenlik sistemleri ve bilgi güvenlik farkındalığı konusundaki gelişmeleri incelemiştir. Bu konuda hedef kitlenin hem uygulama yaparak hem de davranışsal olarak eğitilmesi gerektiğini savunmuştur.

Katsikas (2000:129-135), sağlık kurumlarında personellerin bilgi güvenliği farkındalıklarının sağlanması için uygulanabilecek eğitim alternatifleri sunmuştur. Personellerin ve yöneticilerin teknik ve teorik olarak eğitilmesinin faydalı olacağını savunmuştur.

Rezgui ve Marks (2008:241-253), bilgi güvenlik farkındalığı konusunu yükseköğretimdeki öğrencilerin sorumluluk duygusu, kültürel varsayımlar, inançlar, üniversitelerdeki sosyal şartlar ve personelin öğrenciye davranış türleri ile incelemişlerdir. Beder (2015), ortaokul öğrencilerinin internet kullanımlarını ve bilgi güvenlik farkındalıklarını incelemiştir. Sonuç olarak, öğrencilerin konu hakkında bilinç düzeylerinin yüksek olduğunu tespit etmiştir. Ayrıca bilinç düzeyinin kızlarda ve yaşı büyük olanlarda daha yüksek olduğu sonucuna ulaşmıştır.

Bulgurcu ve diğerlerine göre (2010:523-548) organizasyonlarda bilgi güvenliği, personeller ile işletme arasındaki en zayıf bağ olarak görülmektedir. Bu kapsamda, çalışmada bilgi güvenliği talimatları karşısında çalışanların itaatkâr davranışlarının nasıl sağlanacağı ile ilgili öneriler sunmuşlardır.

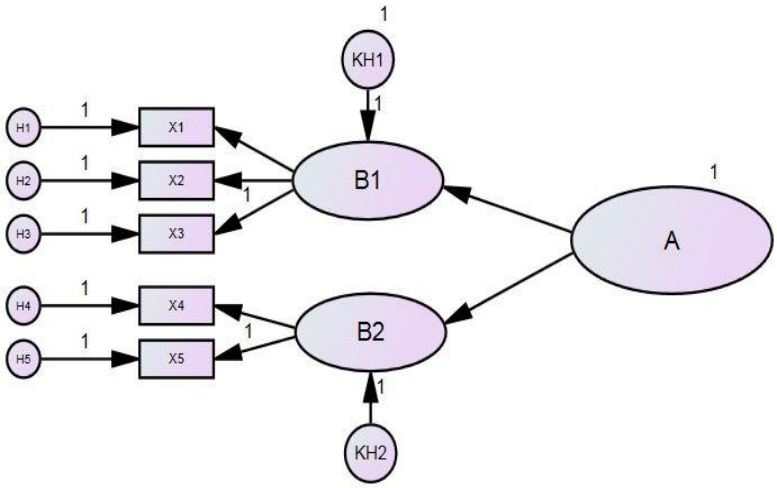
Chung vd. (2008:424-429) çalışmalarında yönetim açısından bilgi güvenlik farkındalığı ile davranış türlerini karşılaştırmışlar ve işletmedeki bilgi güvenlik farkındalığının yönetimin kararlarını olumlu etkilediği sonucuna ulaşmışlardır.

II. YÖNTEM

Yapısal eşitlik modellemesi (YEM); gözlenen, gizil ve bağımlı değişkenler arasındaki nedensel ilişkilerin sınanmasında kullanılan bir istatistiksel yöntem olup, esas çıkış noktası tutumların ölçümüdür (Şahin vd. 2008:153-162). Genellikle teorik gerçeğe veya varsayıma dayalı var olan modelin test edilmesi amacıyla psikoloji, sosyoloji, ekonomi, pazarlama ve eğitim bilimlerinde sıklıkla kullanılmaktadır.

Yöntem yol analizi, doğrulayıcı faktör analizi ve yapısal regresyon analizi olmak üzere üç analiz türünü içermektedir. Yol analizi, Sewall Wright (1922:330-338) tarafından bulunmuş olup, değişkenler arasındaki lineer ilişkinin açıklanabileceği düşüncesine göre ortaya çıkmıştır. Doğrulayıcı faktör analizi ise teorik temele veya varsayıma dayanan bir modelin doğruluğunun test edilmesinde kullanılmaktadır. Doğrulayıcı faktör analizi kısmına ölçüm modeli, yapısal regresyon kısmına yapısal model denilmektedir.

Ölçüm modelinde gözlenen değişkenler ile gizil değişkenler arasındaki ilişki tanımlanmaktadır. Bu kısımda bütün değişkenler serbest bırakılır ve modelin hangi gözlenen değişken ile ne kadar doğru ölçüldüğü belirlenir. Yapısal modelde ise gizil değişkenler ile bağımlı değişken arasındaki nedensel ilişki tespit edilir.



Şekil: 1
YEM diyagramı

Yukarıdaki şekilde yapısal eşitlik modelinin genel yapısı verilmektedir. Bunlardan;

H: Gözlenen değişkenlere ait gözlem hatasını,

X: Gözlenen değişkeni,

B: Gizil değişkeni

KH: Gizil değişkene ait ölçüm hatasını,

A: Bağımlı değişkeni,

A ile B arasındaki yol yapısal regresyon analizi sonucunu,

B ile X arasındaki yol doğrulayıcı faktör analizi sonucunu ifade etmektedir.

AMOS yazılımında YEM uygulaması aşağıdaki adımlara göre yapılmaktadır;

- Şekil 1'e benzer olarak teorik modeli temsil eden diyagramın çizilir,
- Program üzerinde analiz yapıp uyum iyiliğine bakılır,
- İstenilen uyum iyiliğine ulaşılmışsa analize son verilir ve sonuç yorumlanır, aksi halde birbiri ile ilişkili olabileceği düşünülen gözlenen değişkenler modele tanımlanır.

Bu aşamalardan sonra kabul edilebilir uyum iyiliğine sahip olduğu düşünülen YEM modeli sonuçları yorumlanır ve bulgular tartışılır. Model uyum iyiliğini ölçmek amacıyla çoğunlukla kullanılan indeksler aşağıdaki gibidir.

Genel uyum indeksi

(Chi-square goodness of fit) Ki-Kare uyum testi: model ile veriler arasındaki farkı test eder. Bu testin anlamlı olmaması arada bir farkın olmadığını ifade eder, bu durumda modelin uygun olduğu kabul edilmektedir. Ki kare değeri ne kadar küçükse aradaki fark da o kadar küçüktür. Bazı durumlarda ki-kare testinin aksine serbestlik derecesi (SD) yüksek olmasına rağmen test anlamlı çıkabilmektedir. Bu durumda Ki-kare değeri/SD değeri 3'ten küçük olması ki-kare anlamlı dahi olsa modelin uyumlu olduğunu göstermektedir.

Karşılaştırmalı uyum indeksi

Normed Fit Index (NFI) Normlaştırılmış uyum indeksi: test edilen modelin ki kare değerinin, bağımsız modelin ki kare değerine bölünmesiyle elde edilir. İndeks 0 ile 1 arasında değer alır.

Non Normed Fix Index (NNFI) Normlaştırılmamış uyum indeksi: NFI'ya serbestlik derecesi eklenerek elde edilen bir indekstir. Bu indeksi örneklem sayısı küçük olanlarda kullanmak daha doğru sonuçlar verdiği gözlemlenmektedir.

Incremental Fit Index (IFI) Artırmalı uyum indeksi: çok fazla değişken olduğu durumlarda kullanılır. NNFI'ya benzer olup aralarındaki tek fark serbestlik derecesini göz ardı etmesidir.

Mutlak uyum indeksi

Goodness of Fit Index (GFI) uyum iyiliği indeksi: 0 ve 1 arasında değerler alır ve çoğunlukla tercih edilen bir indekstir.

Adjusted Goodness of Fit Index (AGFI) Düzeltilmiş iyilik uyum indeksi: Örneklem genişliği dikkate alınarak hesaplanmış GFI değeridir. 0 ile 1 arasında değerler alır.

Koruyucu uyum indeksleri

Parsimony Normed Fit Index (PNFI): NFI'nın serbestlik derecesi oranı ile çarpılması ile elde edilir. 0 ile 1 arasındadır ve 1'e yaklaştıkça uyum iyiliği arttığı kabul edilir.

Parsinomy Goodness of Fit Index (PGFI): GFI'nın serbestlik derecesi oranı ile çarpılması ile elde edilir. 0 ile 1 arasında değer almakta olup 1'e yaklaştıkça uyum iyiliği artmaktadır.

Artık temelli uyum indeksi

Root Mean Square Residual (RMR) Ortalama hataların karekökü: Korelasyonlar arasındaki farkların karelerinin aritmetik ortalamasının kareköküdür. 0 ile 1 arasında değer alır. 0'a yaklaştıkça uyum iyiliği artmaktadır.

Model karşılaştırma uyum indeksi

Akaike Information Criterion (AIC) Akaike bilgi kriteri: Temel amacı eldeki veriler ile gerçeğe en yakın modeli seçebilmektir. Bu durumda en düşük AIC indeks değerine sahip model gerçeğe en yakın olduğu kabul edilir.

Consistent Akaike Information Criterion (CAIC) Tutarlı Akaike Bilgi Kriteri: örneklem uzayındaki eleman sayısının sonsuza gittiği düşüncesine göre hesaplama esasına dayanmaktadır. En düşük CAIC değerine sahip olan model gerçeğe en yakın olan modeldir.

Excepted Cross Validation Index (ECVI) beklenen çapraz doğrulama indeksi: Birden çok modeli kendi içerisinde karşılaştırır. Amaç kovaryans matrisleri arasındaki uyumsuzluğu incelemektir. Buna göre en düşük ECVI değerine sahip model gerçeğe en yakın olan modeldir.

Tablo: 1
Model Uyum İyilikleri

Ölçümler	***İyi uyum (ARALIKLAR)***	***Kabul edilebilir uyum***
Genel Model Uyumu		
X^2 uyum indeksi	Anlamlı olmaması durumu ($p<0,05$)	-
Karşılaştırmalı model uyumu		
X^2/SD	0-3	3-5
NFI	1-0,95	0,90-0,94
NNFI	1-0,95	0,90-0,94
IFI	1-0,95	0,90-0,94
CFI	1-0,97	0,95-0,96
RMSEA	0-0,05	0,06-0,08
Mutlak uyum indeksleri		
GFI	0,90-1	0,85-0,89
AGFI	0,90-1	0,85-0,89
Koruyucu uyum indeksleri		
PNFI	0,95-1	
PGFI	0,95-1	
Artık temelli uyum indeksleri		
RMR	0-0,05	0,05-0,08
Model karşılaştırmalı uyum indeksleri		
AIC	En küçük değerli model	
CAIC	En küçük değerli model	
ECVI	En küçük değerli model	

III. AMAÇ, KAPSAM VE METOT

Çalışmada yüksekokul öğrencilerinin bilgi güvenlik farkındalıklarını etkileyen faktörleri ve bu faktörlerin etki düzeylerinin belirlenmesi amaçlanmaktadır. Bu kapsamda çalışmanın evrenini Çukurova Üniversitesi Kozan Meslek Yüksekokulunda öğrenim gören öğrenciler oluşturmaktadır.
Yüksekokulda; Bankacılık ve Sigortacılık (1. ve 2. öğretim), Muhasebe (1. ve 2. öğretim), Büro Yönetimi ve Yönetici Asistanlığı (1. ve 2. öğretim), Yerel Yönetimler (1. öğretim), Tohumculuk (1. öğretim), Mobilya ve Dekorasyon (1. öğretim), Bahçe Tarımı (1. öğretim), Bilgisayar (1. ve 2. öğretim) sınıfları bulunmaktadır. Bu sınıflardan kotalı örnekleme yöntemiyle ikili öğretim veren ve sınıf kontenjanı 50 olan bölümlerde 35'er kişi, sınıf kontenjanı 35 olan

bölümlerde ise 25'er kişi rastgele seçilmiş olup toplamda 420 öğrenci çalışmanın örneklemini oluşturmaktadır.
Çalışmada kullanılan anket, Parsons vd. (2013) tarafından geliştirilen HAIS-Q ölçeğinden 5'li Likert ölçeğe (1:Kesinlikle Katılmıyorum, 2: Katılmıyorum, 3: Kararsızım, 4: Katılıyorum, 5: Kesinlikle Katılıyorum) göre uyarlanmıştır. Bu yöntemle elde edilen veri seti ile öncelikle katılımcılara ait tanımlayıcı istatistikler oluşturulmuştur. Daha sonra keşfedici faktör analizi ve yapısal eşitlik modeli uygulaması yapılmıştır.

Çalışmanın analiz kısmı, öğrenciler ile ilgili tanımlayıcı istatistiklerin ardından verilerin ve modelin, geçerlilik ve güvenirlik analizleri ile yapısal regresyon analizini içermektedir. Yapısal eşitlik modeli uygulaması IBM Amos programı ile tanımlayıcı istatistikler SPSS 22,0 ile yapılmıştır.

A) Tanımlayıcı İstatistikler

Ankete katılanların %63,8'i bay %36,2 si ise bayan olup bunların da %70'i 19 ile 25 yaşları arasındadır. Öğrencilerin %85,5'i kişisel bilgisayara sahip olup, %50'si kablosuz internet aracılığıyla veya cep telefonları ile internete girmektedirler. %63,6'sı kişisel şifrelerini çalındığını düşündüklerinde veya şifresini birisine verdiklerinde değiştirmektedirler. Ayrıca %95'i evde, okulda veya yurtta internete girmektedirler.
Öğrencilerin %57,6'sı 1 saat ile 3 saat arasında internete girmektedir ve sosyal ağ sitelerinde genellikle 1 saatten fazla zaman geçirmektedirler. E-devlet şifresi olanlar %57,4 olup internet bankacılığı kullananlar %59,3; internet üzerinden alış veriş yapanlar %55,2'dir.
Halka açık internetin olduğu yerlerde bağlantı kurmayı güvenlik açısından riskli görenlerin oranı %57,1'dir. Öğrencilerden internet ortamında iletişim bilgilerimi paylaşırım diyenler %43,8'dir. %88,3'ü internet üzerinden dosya aktarımını e-posta veya sosyal ağ siteleri aracılığı ile yapmaktadır, özel şifre programı kullananların oranı ise %68,6'dir.

B) Keşfedici Faktör Analizi Uygulaması
Ankette tanımlayıcı istatistikler ile ilgili sorular hariç 30 adet soru bulunmaktadır. Bu sorunların tamamının alfa güvenirlik katsayıları 0,831 olarak bulunmuştur. Bu ise verilerin %83,1 oranında güvenilir olduğunu göstermektedir.

Tablo :2
Güvenirlik Analizi Sonucu

Cronbach Alfa	Soru Sayısı
0,831	30

Keşfedici faktör analizinde faktör çıkarma yöntemi olarak temel bileşenler analizi, döndürme metodu olarak promax tercih edilmiştir. Buna göre 6 soru birden fazla faktörle ilişkili olduğu sonucuna ulaşılmış ve bu sorular çıkartılmıştır. Bunların ardından elde edilen sonuçlar aşağıdaki gibidir.

Tablo: 3
KMO-Bartlett Testi Sonucu

Kaiser-Mayer-Olkin Örneklem Yeterliliği Ölçümü		,817
Bartlett Testi	Ki-kare değeri	2421,172
	Serbestlik Der.	276
	Anlamlılık	,000

Tablo 3'e göre KMO testi %81,7 olarak bulunmuş, bu ise verilerin örneklem büyüklüğünün yeterli olduğunu göstermektedir. Bartlett testinin anlamlı olması verilerin faktör analizine uygun olduğunu göstermektedir. Buna göre veriler faktör analizine uygun bulunmuş ve keşfedici faktör analizi uygulaması yapılmıştır.

Tablo: 4
Faktör Analizi Sonucu

Açıklanan Toplam Varyans							
	Başlangıç Öz değerleri			Faktör Yüklerinin Karesi			
	Top.	% Vary.	Birikimli	Top.	% Vary.	Birikimli	Top.
1	4,997	20,822	20,822	4,997	20,822	20,8	3,98
2	2,601	10,837	31,660	2,601	10,837	31,6	3,50
3	1,623	6,762	38,422	1,623	6,762	38,4	2,35
4	1,252	5,218	43,640	1,252	5,218	43,6	2,11
5	1,156	4,816	48,455	1,156	4,816	48,4	2,42
6	1,124	4,683	53,139	1,124	4,683	53,1	1,72
7	,987	4,112	57,251				
8	,920	3,832	61,083				
9	,903	3,761	64,844				
10	,826	3,440	68,285				
11	,778	3,243	71,528				
12	,726	3,027	74,555				
13	,688	2,866	77,421				
14	,650	2,708	80,129				
15	,629	2,622	82,751				
16	,597	2,487	85,238				
17	,577	2,405	87,643				
18	,525	2,187	89,830				
19	,518	2,160	91,990				
20	,473	1,969	93,959				
21	,422	1,759	95,718				
22	,384	1,598	97,316				
23	,347	1,445	98,761				
24	,297	1,239	100,000				
Faktör Çıkarım Metodu: Temel Bileşenler Analizi							

Tablo 4'e göre anket soruları 6 faktör altında toplanabilmektedir ve bu faktörler bilgi güvenlik farkındalığı sorunsalını toplam %53,1 oranında açıklamaktadır. Faktör analizinde anlamlı bir ölçek geliştirebilmek amacıyla faktörlere döndürme işlemi yapılmaktadır. Bu durumda promax döndürme fonksiyonuna göre elde edilen sonuçlar aşağıdaki gibidir.

Tablo :5
Döndürülmüş Faktör Yükleri

	Bileşen					
	F1	F2	F3	F4	F5	F6
S28	,841					
S27	,736					
S29	,678					
S22	,572					
S21	,445					
S30	,429					
S12		,691				
S13		,657				
S1		,640				
S16		,618				
S4			,708			
S2			,708			
S3			,638			
S6			,526			
S14				,761		
S15				,683		
S5				,620		
S9					,735	
S10					,600	
S8					,462	
S7					,435	
S26						,771
S24						,635
S18						,482

Tablo 5'e göre birinci faktör bilgi yönlendirme ve koruma özelliklerini ölçmeye yönelik 6 maddeden, ikinci faktör bilgisayar sistem güvenliği algısını ölçmeye yönelik olarak 4 maddeden, üçüncü faktör şifre yönetimine yönelik 4 maddeden, dördüncü faktör sosyal ağ siteleri ve kişisel tehditlere yönelik 3 maddeden, beşinci faktör e-posta ve internet kullanımına ait 4 maddeden ve altıncı faktör mobil internet kullanımına yönelik 3 maddeden oluşmaktadır. Ayrıca temel bileşenler analizine göre 30 sorudan 6 tanesi birbiri ile benzer şeyi ölçtüklerinden ve faktör yükleri 0,4'ten düşük oldukları görüldüğünden analiz dışında tutulmuştur.

Bu faktörlerin isimlendirilmesinin aşağıdaki gibi olması uygun görülmüştür.

F1: Bilgi Yönlendirme ve Koruma Özellikleri (%20,82)

F2: Bilgisayar Sistem Güvenliği (%10,83)

F3: Şifre Yönetimi (%6,76)

F4: Sosyal Ağ Siteleri ve Kişisel Tehditler (%5,21)

F5: E posta ve İnternet Kullanımı (%4,81)

F6: Mobil İnternet Kullanımı (%4,68)

C) Araştırmanın Hipotezleri ve Modeli

Yüksekokul öğrencilerinin bilgisayar kullanım alışkanlıkları ile bilgi güvenlik farkındalıkları arasındaki nedensellik ilişkisini araştırmak amacıyla aşağıdaki hipotezler test edilmiştir.

H_1: Bilgi yönlendirme ve koruma davranışları ile bilgi güvenlik farkındalığı arasında anlamlı bir ilişki vardır.

H_2: Bilgisayar sistem güvenliği ile bilgi güvenlik farkındalığı arasında anlamlı bir ilişki vardır.

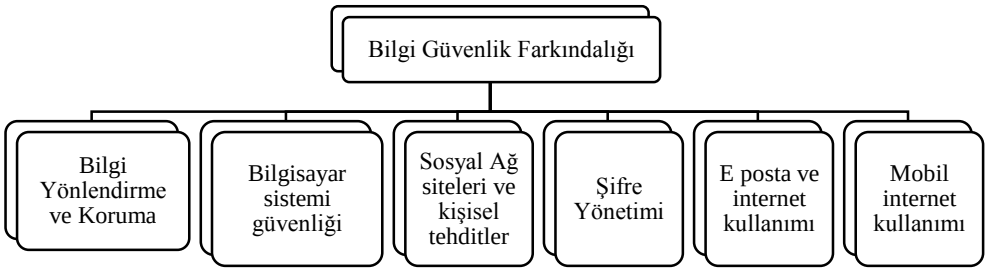
H_3: Şifre Yönetimi ile bilgi güvenlik farkındalığı arasında anlamlı bir ilişki vardır.

H_4: Sosyal ağ siteleri kullanımı ve kişisel tehditler ile bilgi güvenlik farkındalığı arasında anlamlı bir ilişki vardır.

H_5: E posta ve internet kullanımı ile bilgi güvenlik farkındalığı arasında anlamlı bir ilişki vardır.

H_6: Mobil internet kullanımı ile bilgi güvenlik farkındalığı arasında anlamlı bir ilişki vardır.

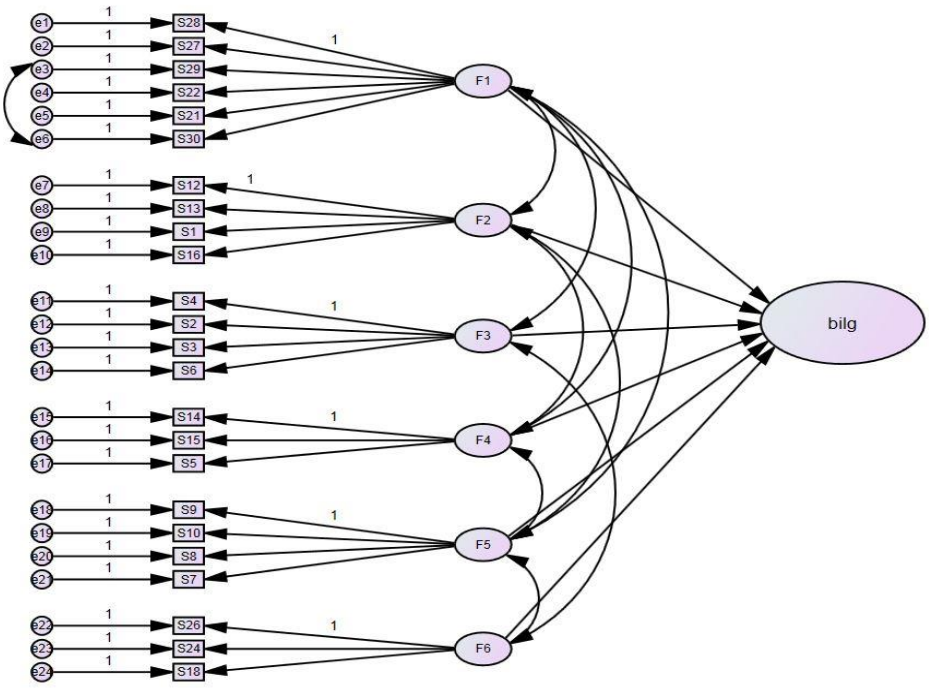
Bilgi güvenlik farkındalığına ilişkin önerilen teorik modelin grafiği aşağıdaki şekilde verilmiştir.



Şekil: 2
Araştırma Modeli

D) Yapısal Eşitlik Modeli Uygulaması

Yapısal eşitlik modeli doğrulayıcı faktör ve yapısal regresyon analizinin birlikte uygulanmasıdır. Buna göre öncelikle faktörlere ve anket sorularına bir önceki aşamada elde edilen faktör analizi sonuçlarına göre doğrulayıcı faktör analizi uygulanmıştır. Yapısal regresyon analizi uygulamasında literatürde genel kabul görmüş ve yoğun kullanılan bir teknik olan Maksimum Likelihood (ML) yöntemi tercih edilmiştir.



Şekil: 3
Yapısal Eşitlik Modeli Uygulama Grafik Görünümü

Amos programına girilerek elde edilen yol grafiği şekil 3'de gösterilmektedir. İyileştirme indislerine göre 29 ve 30 nolu soruların birbiri ile ilişkili olduğu sonucuna ulaşılmıştır. Bu nedenle bu soruların hatalarını ifade eden diyagramlar birbiri ile ilişkilendirilmiştir.

Tablo: 6
Doğrulayıcı Faktör Analizi Sonuçları

	Sorular	Faktör Yükleri	Anlamlılık
Bilgi yönlendirme ve Koruma Özellikleri	S30 Bilgisayarlarda izinsiz başkalarının bilgilerini okumanın suç olduğunu	,537	
	S29 Bir sitenin benim bilgi güvenliğimi tehdit edip etmediğini anlarım.	,672	***
	S28 İhtiyaç halinde şifremi arkadaşlarımla paylaşırım.	,636	***
	S27 Şifre gerektiren bütün işlemlerde genellikle aynı şifreyi kullanırım.	,429	***
	S22 Bilgi güvenliğim için ücret ödeyip bir koruma programı satın alırım.	,710	***
	S21 Okulumda uygun olmayan web sitelerine erişimi engellemeye yönelik program kullanılıyor.	,656	***
Bilgisayar Sistem Güvenliği	S1 İhtiyaç halinde arkadaşlarımın kişisel bilgisayarımı kullanmasına izin veririm.	,371	
	S12 Ücretsiz sürümü biten programı bilgisayarımdan silerim.	,585	***
	S13 İzinsiz müzik, video indirme programları kişisel bilgilerimi tehdit eder.	,684	***
	S16 Bilgisayarımda devamlı bir anti virüs programı aktiftir.	,608	***
Şifre Yönetimi	S2 Bilgisayarımda her türlü bilgiler kayıtlıdır, bu da beni tedirgin eder.	,532	
	S3 Sanal sohbet ederken, gerçek bilgilerimi saklamaya özen gösteririm.	,586	***
	S4 Sanal sohbet ettiğim kişiye inanıp inanmamakta tereddüt ederim.	,612	***
	S6 İnternet üzerinden kredi kartıyla alışveriş yaparım.	,405	***
Sosyal Ağ siteleri Ve Kişisel Tehditler	S5 Sohbet metinlerinin başka kişiler tarafından okunabileceğini biliyorum.	,433	
	S14 Başka bilgisayarda internete girdikten sonra kayıtlı bir şey olup olmadığına dikkat ederim.	,541	***

	S15 Bilgisayarımda internet gezinti bilgilerini silen bir program devamlı aktiftir.	,838	***
E posta ve internet Kullanımı	S7 Kredi kartı bilgilerimin çalınacağından tereddüt ederim.	,540	
	S8 Sanal alışveriş daima bir risktir, kolay kolay güvenmem.	,509	***
	S9 İnternette gezinirken bilmediğim kişiler tarafından rahatsız ediliyorum.	,419	***
	S10 Müzik, video, program veya dosya paylaşımı için özel site veya program kullanırım	,271	***
Mobil İnternet Kullanımı	S18 Benim için önemli bir dosyaları birden fazla yere kaydederim.	,497	
	S24 Her an bilgilerin kaybolma ihtimali için dosyalarımı yedeklerim.	,518	***
	S26 Bilgi güvenliği ile alakalı yeterli bilgiye sahibim.	,580	***

Tablo 6'ya göre S22, S29, S28, S21, S13, S16, S4 ve S15'inci maddeler faktör yükleri en yüksek olanlardır. Ayrıca yol analizine göre yorumlandığında; gözlenen değişkenler (anket soruları) ile faktörler arasındaki yolların tamamının anlamlı olduğu, dolayısıyla soruların doğru faktör altında açıklandığı görülmektedir. Faktörlerin belirlenmesinin ardından yapısal regresyon analizinde çoklu bağlantı problemine karşı faktörler arasında korelasyon analizi uygulanmıştır.

Tablo: 7

Korelasyon Analizi Sonucu

Korelasyon Tablosu							
		F1	F2	F3	F4	F5	F6
F1	Korelasyon	1					
	Anlamlılık						
F2	Korelasyon	,360	1				
	Anlamlılık	,000					
F3	Korelasyon	,371	,094	1			
	Anlamlılık	,000	,055				
F4	Korelasyon	-,022	,056	,185	1		
	Anlamlılık	,650	,251	,000			
F5	Korelasyon	-,212	-,082	-,169	-,152	1	
	Anlamlılık	,000	,095	,001	,002		
F6	Korelasyon	-,112	-,070	-,104	-,018	,210	1
	Anlamlılık	,021	,149	,033	,706	,000	

Tablo 7'ye göre faktörler arasında birbiri ile yüksek korelasyon ilişkisi bulunmamakta olup çoklu bağlantı sorunu olmadığı sonucuna ulaşılmaktadır. Gizil değişkenler ile bağımlı değişken arasındaki yapısal regresyon analizi sonuçlarına göre test edilen hipotezler ve anlamlılıkları aşağıdaki gibidir.

Tablo: 8
Yapısal Regresyon Analizi Sonuçları

	Test Edilen Hipotez	Beta	Anlamlılık	Kabul/Ret
H_1	Bilgi yönlendirme ve koruma davranışları ile bilgi güvenlik farkındalığı arasında anlamlı bir ilişki vardır.	,258	***	**Kabul**
H_2	Bilgisayar sistem güvenliği ile bilgi güvenlik farkındalığı arasında anlamlı bir ilişki vardır.	,216	***	**Kabul**
H_3	Şifre Yönetimi ile bilgi güvenlik farkındalığı arasında anlamlı bir ilişki vardır.	,324	***	**Kabul**
H_4	Sosyal ağ siteleri kullanımı ve kişisel tehditler ile bilgi güvenlik farkındalığı arasında anlamlı bir ilişki vardır.	,263	***	**Kabul**
H_5	E posta ve internet kullanımı ile bilgi güvenlik farkındalığı arasında anlamlı bir ilişki vardır.	,264	***	**Kabul**

H_6	Mobil internet kullanımı ile bilgi güvenlik farkındalığı arasında anlamlı bir ilişki vardır.	,296	***	**Kabul**
*** **Testin %5 hata payına göre anlamlı olduğunu göstermektedir.**				

Elde edilen regresyon analizi sonuçlarına göre gizil değişkenlerin tamamının bilgi güvenlik farkındalığını etkilediği doğrulanmış olup test edilen bütün hipotezler kabul edilmiştir. Buna göre öğrencilerin bilgi yönlendirme ve koruma davranışlarındaki 1 birimlik pozitif yönlü değişim, bilgi güvenlik farkındalığında 0,258 birim artışa neden olmaktadır. Diğer faktörler de benzer şekilde değerlendirildiği durumda bilgi güvenlik farkındalığını en çok etkileyen faktör şifre yönetimi olduğu görülmektedir. Bu faktörü sırasıyla mobil internet kullanımı, e posta ve internet kullanımı, sosyal ağ kullanımı, bilgi yönlendirme ve bilgisayar sistem güvenliği takip etmektedir. Dolayısıyla bu sonuca göre öğrencilerin bilgi güvenlik farkındalıklarını geliştirebilmek için öncelikle şifre yönetimi konusunda bilgiler verilmesi gerektiği ifade edilebilir.

E) Model Uyum İyiliği

Yapısal eşitlik modeli uygulamasının en önemli yanlarından bir tanesi de önerilen modelin veri seti ile uyumlu olup olmadığının sınanmasıdır. Model uyum iyiliği, literatürde savunulan model ile verilerden elde edilen model arasındaki farkı ölçmeye dayanır. Bunun için daha önce belirtildiği üzere çok farklı yöntemler ve değerler olmasına rağmen genel kabul görmüş beş model uyum iyilik indisleri bulunmaktadır. Bu indislere ilişkin sonuçlar aşağıdaki gibidir.

Tablo:9
Model Uyum İyilik Skorları

Uyum iyiliği	Mükemmel Uyum İyiliği	Kabul edilebilir	Elde edilen skor	Sonuç
P değeri	<0,01	-	0,000	Mükemmel
CMIN/DF	0-3	3,5	2,39	Mükemmel
RMR	0-0,05	0,05-0,1	0,1	Kabul Edilebilir
GFI	1-0,95	0,95-0,90	0,92	Kabul Edilebilir
IFI	1-0,95	0,95-0,90	0,90	Kabul Edilebilir
RMSEA	0-0,05	0,05-0,1	0,04	Mükemmel

Tablo 9'a göre elde edilen skorlar değerlendirildiğinde, uyum iyiliklerinin tamamının kabul edilebilir veya mükemmel uyum iyilikleri sınırında olduğu sonucuna ulaşılır. Bu da verilerin savunduğu model ile teorik olarak elde edilen modelin birbiri ile uyumlu olduğu sonucunu vermektedir.

SONUÇLAR

Bu çalışmada yüksekokul öğrencilerinin bilgi güvenlik farkındalıklarını etkileyen faktörleri ve bu faktörlerin etki düzeylerini belirlemek amaçlanmıştır. Çukurova Üniversitesi Kozan Meslek Yüksekokulu kapsamında yapılan uygulamada 420 kişiye ulaşılmış ve anket yöntemiyle veri seti elde edilmiştir.

Demografik özelliklerin ardından bilgi güvenlik farkındalığı davranışlarını yansıtan anket sorularına yer verilmiş olup bunlara keşfedici faktör analizi uygulaması neticesinde soruların 6 faktör altında toplanmasının uygun olduğuna karar verilmiştir. Bu faktörler bilgi yönlendirme ve koruma özellikleri, bilgisayar sistem güvenliği, şifre yönetimi, sosyal ağ siteleri ve kişisel tehditler, e posta ve internet kullanımı ve mobil internet kullanımıdır.

Faktör analizi ile elde edilen faktör ve bileşenlere doğrulayıcı faktör analizi ve yapısal regresyon analizini içeren yapısal eşitlik modeli uygulanmıştır. Buradan modelin anlamlı olduğu yani faktörlerin doğrulandığı sonucuna ulaşılmıştır. Yapısal regresyon (yol analizi) sonuçlarına göre faktörlerin hepsinin öğrencilerin bilgi güvenlik farkındalıklarını etkilediğini savunan hipotezler kabul edilmiştir. Bu faktörlerden bilgi güvenlik farkındalığını en çok etkileyenler sırasıyla şifre yönetimi, mobil internet kullanımı, e posta ve internet kullanımı ve sosyal ağ sitelerinin kullanım davranışlarıdır. Daha sonra yapılacak çalışmalarda anket ölçeğini geliştirerek veya farklı örnekleme uygulayarak sonuçların karşılaştırılması önerilebilir.

KAYNAKÇA

BULGURCU, B., ÇAVUŞOĞLU, H. ve BENBASAT, I. (2010) "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs And İnformation Security Awareness." MIS, 34(3), 523-548.

CHUNG, M., CHOI, J., YANG, S. ve RHYOO, S. K. (2008) "Context-Aware Security Services in DAA Security Model in Advanced Language Processing and Web Information Technology", 2008. ALPIT'08. International Conference on (ss. 424-429). IEEE.

GÖKMEN, Ö. F., AKGÜN, Ö. E. (2015). "Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Eğitimi Verebilmeye Yönelik Yeterlilik Algılarının İncelenmesi" İlköğretim Online, 14(4).

GÜLER, H., MERAL, O., KOSE, C., TEYİN, A., SENOL, E. ve KOCAK, A. (2015). "A Survey Study on the Use of Internet and Social Networking of the Ege University Medical School Students and Doctors" Medicine Science, 4(1).

HANSCHE, S. (2001). "Making Security Awareness Happen, The Privacy Papers: Managing Technology", Consumer, Employee and Legislative Actions, 51.

KATSIKAS, S. K. (2000). "Health Care Management And Information Systems Security: Awareness, Training or Education?" International journal of medical informatics, 60(2), 129-135.

KEGEL, R. H., WIERINGA, R. J. (2015). "Behavior Change Support Systems for Privacy and Security" In Proceedings of the Third International Workshop on Behavior Change Support Systems (BCSS2015), Chicago, USA, June (Vol. 3).

KRUGER, H. A., KEARNEY, W. D. (2006). "A Prototype for Assessing Information Security Awareness" Computers & Security, 25(4), 289-296.

PARSONS, K., MCCORMAC, A., BUTAVİCİUS, M., Pattinson, M. ve Jerram, C. (2013). "The Development of the Human Aspects of Information Security Questionnaire (HAIS-Q)" In 24th Australasian Conference on Information Systems (ACIS) (pp. 1-11). RMIT University.

PFLEEGER C. P. (1997), "The Fundamentals of Information Security" IEEE Software, 14(1)

REZGUİ, Y., MARKS, A. (2008). "Information Security Awareness in Higher Education: An Exploratory Study". Computers & Security, 27(7), 241-253.

SALEH, M. S., ALFANTOOKH, A. (2011). "A New Comprehensive Framework for Enterprise Information Security Risk Management" Applied Computing and Informatics, 9(2), 107-118.

SHAMALA, P., AHMAD, R. ve YUSOFF, M. (2013). "A Conceptual Framework of info Structure for Information Security Risk Assessment (ISRA)" Uluslararası Güvenlik ve Uygulamaları Dergisi, 18(1), 45-52.

SIPONEN, M., MAHMOOD, M. A. ve PAHNILA, S. (2014). "Employees' Adherence to Information Security Policies: An Exploratory Field Study" Yönetim ve Bilgi Dergisi, 51(2), 217-224.

ŞAHİN, A., CANKURT, M., GÜNDEN, C. ve MİRAN, B. (2008). "Çiftçilerin risk davranışları: Bir yapısal eşitlik modeli uygulaması" Dokuz Eylül Üniversitesi, İİ BF Dergisi, 23(2), 153-172.

TEKEREK M. (2008) "Bilgi Güvenliği Yönetimi" KSÜ Fen ve Mühendislik Dergisi, 11(1) ss.132:138

TEKEREK, M., TEKEREK, A. (2013). "A Research on Students' Information Security Awareness" Türkçe Eğitim Dergisi, 2(3).

TSOHOU, A., KARYDA, M., KOKOLAKIS, S. ve KIOUNTOUZIS, E. (2015). "Managing the Introduction of Information Security Awareness Programmes in Organisations" European Journal of Information Systems, 24(1), 38-58.

WRIGHT, S. (1922). "Coefficients of Inbreeding and Relationship. The American Naturalist", 56(645), 330-338.

YANG, Y. P. O., SHIEH, H. M. ve TZENG, G. H. (2013) "A VIKOR Technique Based on DEMATEL and ANP for Information Security Risk Control Assessment" Information Sciences, 232, 482-500.