K. Ü. Kastamonu Eğitim Dergisi, 23 (3), 1167-1184

Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması

Development Of Information Security Awareness Scale

Hafize KESER, Can GÜLDÜREN
Ankara Üniversitesi, Eğitim Bilimleri Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Cebeci, Ankara

Makalenin Geliş Tarihi: 14.12.2014 ***Yayına Kabul Tarihi: 31.05.2015***

Özet

Bu çalışmanın amacı, yükseköğretim kurumlarında çalışan öğretim elamanlarının bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirmektir. Araştırma, Türkiye'de çeşitli yükseköğretim kurumlarında görev yapan 363 öğretim elemanıyla gerçekleştirilmiştir. Açımlayıcı faktör analizi sonucunda, ölçeğin 34 madde ve 2 alt boyuttan (''saldırı ve tehditler'' ile ''kişisel verilerin korunması'') oluştuğu belirlenmiştir. Katılımcılar arasından rastgele seçilen 200 kişilik grup üzerinde yapılan doğrulayıcı faktör analizi sonucunda 2 faktörlü yapı doğrulanmıştır. Ölçeğin tamamı için Cronbach alfa güvenirlik katsayısı .97; her alt boyut için sırasıyla.97 ile .94'tür. Bu çalışma sonucunda yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerini belirlemek için kullanılabilecek geçerli ve güvenilir bir ölçek geliştirilmiştir.

Anahtar Kelimeler: *Bilgi, güvenlik, farkındalık, bilinçlendirme, bilgi güvenliği, ölçek geliştirme.*

Abstract

The purpose of the this study is to develop an ''information security awareness scale'' for faculty members to determine the level of information securty awareness. The study was conducted with 363 faculty members working in various higher education institutions in Turkey. As a result of exploratory factor analysis, it was determined that the scale consists of 34 items and 2 subscales ('attacks and threats' and 'the protection of personal data'). Confirmatory factor analysis was conducted with randomly selected group of 200 academicians among participants. Two-factor structure was confirmed. Cronbach's alpha reliability coefficient is .97 for the entire scale; .94, .97, respectively, for each subscale. Consequently in this study, a valid and reliable instrument that can be used to determine the level of information security awareness of faculty members has been developed.

Keywords: *Information, security, awareness, awareness raising, information security, scale development.*

1. Giriş

Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişimini, kullanımını, değiştirilmesini, ifşa edilmesini, ortadan kaldırılmasını, el değiştirmesini ve hasar verilmesini önlemek olarak tanımlanabilir. Gizlilik, bütünlük ve erişilebilirlik olarak isimlendirilen üç temel unsurdan meydana gelir (Puhakainen, 2006). Bu üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik zafiyeti oluşur. Bilgi güvenliği kurumlar ve bireyler için vazgeçilmez ve değerli bir varlık olan bilginin korunması için gerekmektedir. Bu konuyla ilgili bir diğer husus ise bilginin işlenmesi için kullanılan ve sürekli gelişim gösteren teknolojilerin de bilgi unsuru için riskler yarattığı gerçeğidir.

Bilgi ve iletişim teknolojisinin yaygınlaşması, Internet'in yaygın olarak kullanılması ve Internet üzerinde kullanılan çevrimiçi uygulamalardaki artış, paralelinde güvenlik açıklarının artışına sebep olur iken bilgi güvenliğini sağlamak toplumda sadece bilgi güvenliğinden sorumlu kişi ve kuruluşların işi olmaktan çıkmıştır (Acılar, 2009; Tsohou, Kokolakis, Karyda ve Kiountouzis, 2008; Vural ve Sağıroğlu, 2011). Günümüzde, bilgi sistemlerinin küreselleşmesi sonucunda bu sistemlerle doğrudan veya dolaylı yönden ilişkili olan ve bu sistemleri kullanan tüm birey ve kurumların artık bilgi güvenliğine katkıda bulunması gerekmektedir (Özcan, 2009; Vardal, 2009; Vural ve Sağıroğlu, 2011).

Bilgi güvenliği risklerinden korunmanın en iyi yolu bilgi teknolojilerine çok para harcamak ve korunma amaçlı teknolojileri daha çok kullanmaktan önce, insanların bilinçlenmesi ve ihtiyaç duyulan güvenlik teknolojisini doğru yer ve zamanda kullanmakla mümkün olabilir (Puhakainen, 2006; Siponen, 2001; Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009). İnsan faktörüne bağlı bilgi güvenlik risklerini hiçbir zaman tamamen ortadan kaldırmak mümkün olmasa da, iyi planlanmış bir farkındalık etkinliği ile güvenlik risklerinin kabul edilebilir bir seviyeye çekilmesi sağlanabilir (Acılar, 2009; Gülmüş, 2010; Kruger ve Kearney, 2006; Şahinaslan, Kandemir ve Şahinaslan, 2009; Vardal, 2009; Vural, 2007).

Bilgi ve iletişim teknolojileri ile birlikte geliştirilen elektronik uygulamalar bir yandan hayatın işleyişini kolaylaştırırken diğer yandan yeni güvenlik tehditlerini ve yeni suç tiplerini beraberinde getirmektedir (Gülmüş, 2010). Son 15-20 yılda bilgi güvenliğine olan ilgi, dünyada olduğu gibi ülkemizde de çok büyük bir artış göstermiş ve buna paralel olarak bu alanda ülkemizde yapılan araştırmalarda artmıştır. Bilgi güvenliği konusundaki araştırmalar, problemleri daha çok teknik bakış açısıyla ele alıp, insan faktörünü göz ardı etmektedir (Chen, Shaw ve Yang, 2006; Kjorvik, 2010; Rezgui ve Marks, 2008). Kurumsal ve kişisel bilgilerin güvenliğini sadece teknik güvenlik önlemleriyle (güvenlik duvarı, sanal özel ağ, saldırı tespit/önleme sistemi, anti virüs, içerik kontrolü yazılımı, veri şifreleme, kimlik doğrulama, yetkilendirme vb.) sağlamak mümkün değildir (Rezgui ve Marks, 2008). Ayrıca, bunun yanında kurum ve çalışanların güvenlik bilincine sahip olması gerekmektedir.

Zaman içerisinde güvenlik teknolojileri geliştirildikçe, olası teknik açıkları kullanmak/sömürmek zorlaştığı için saldırganlar insan unsurunun zayıflıklarından faydalanmaya başlamışlardır. Bu yüzden kurumlarda güvenliğin en zayıf halkasını insan unsuru oluşturmaktadır (Kritzinger ve Smith, 2008; Mahabi, 2010; Mathisen, 2004; Penmetsa, 2010; Veiga, 2008). Genel bir söylem olarak "bir zincir, en zayıf halkası kadar güçlüdür" sözü bilgi güvenliği için de geçerlidir.

Her hangi bir bilgi sisteminde bilginin sahibi, bilgiyi kullanan ya da bilgi sistemini yönetenlerden biri olmak, kişiyi sorumlu kılmaktadır. Bilgi güvenliği seviyesi bu durumda kullanıcılara bağlı olduğundan, kullanıcı farkındalığı bilgi güvenliğinin sağlanmasında son derece kritik bir öneme sahiptir. Alanyazın incelemesiyle elde edilen sonuçlar bilgi güvenliği farkındalığı açısından yükseköğretim kurumlarının çok iyi durumda olmadığına işaret etmektedir (Cox, Connolly ve Currall, 2001; Rezgui ve Marks, 2008; Vardar, 2009). Bilgi güvenliği uzmanlarıyla gerçekleştirilen bir çalışmada yükseköğretim kurumlarının bilişim sistemleri güvenliği açısından dünyadaki en güvensiz yerlerden biri olduğu ifade edilmektedir (Foster, 2004; Rezgui ve Marks, 2008; Mahabi, 2010). Yapılan testler ve denetimler yükseköğretim kurumları bilgi sistemlerinde birçok açığın ve zayıf yanların bulunduğunu göstermektedir (Mahabi, 2010; Rezgui ve Marks, 2008). Bilgi ve bilişim sistemleri güvenliği eğitimleri diğer kurumlarda olduğu gibi yükseköğretim kurumları için de bir zorunluluktur. ABD'de Winsconsin Üniversitesi tarafından 435 yükseköğretim kurumunda uygulanan ankete katılan enstitülerden sadece üçte birinde öğrenci ve personel için bilgi güvenliği farkındalık eğitimi verildiği tespit edilmiştir (Caruso, 2003). Ülkemizdeki durumun bu ankette çıkan sonuçtan daha iyi olmadığını söylemek mümkündür (Vardar,2009).

Bilginin üretiminden, öğretiminden, sunumundan ve dağıtımından sorumlu temel ve öncü kurumlardan olan üniversiteler ve öğretim elemanları bu görevlerini yerine getirirken bilgi güvenliği konusunu ön planda tutmak ve kendilerini bu konuda yetiştirmek zorundadırlar. Bu bağlamda, toplumu ve öğrencileri bilinçlendirme görevi üstlenecek olan öğretim elemanlarının bilgi güvenliği farkındalıklarının hangi düzeyde olduğu, bu konuda eksikliklerinin hangi alanlarda yoğunlaştığının belirlenmesi önem arz etmektedir. Bilgi güvenliği farkındalığıyla ilgili yapılan alanyazın taramasında, yurtdışında bilgi güvenliği farkındalığının ölçülmesiyle ilgili Kruger ve Kearney'in (2006) metodolojik bir yaklaşım ortaya koyan ve uluslararası bir maden şirketi için geliştirmiş oldukları bir çalışmaya ulaşılmıştır. Türkiye'de ise özellikle üniversitelerde görev yapan öğretim elemanlarına yönelik bilgi güvenliği farkındalığıyla ilgili herhangi bir çalışmaya ulaşılamamıştır. Dünya'da ve Türkiye'de yapılan çalışmalar daha çok bilgi güvenliği yönetim sistemleri, risk değerlendirmesi, bilgi güvenliği farkındalık eğitimleri ve bilgi güvenliği sorunlarıyla ilgili durum tespiti konu başlıkları altında toplanmaktadır. Yapılan çalışmalar daha çok genel durum tespitine yönelik iken bilgi güvenliğinde "en zayıf halka" olarak ifade edilen insan unsurunun bilgi güvenliği farkındalık düzeyinin ne olduğunu belirleyecek bir çalışmaya ulaşılamamıştır. Bu araştırma öğretim elemanlarının bilgi güvenliği farkındalık düzeyini belirleyecek olan bir ölçeğinin geliştirilmesi ve ön-psikometrik (preliminary) özelliklerin belirlenmesi amacıyla gerçekleştirilmiştir.

2. Yöntem

Araştırma tarama modelinde gerçekleştirilmiştir. Araştırmanın yürütülmesi için gerekli olan etik kurulu kararı alınmıştır.

Çalışma Grubu. Araştırma grubunu, Türkiye'de 40 farklı üniversitede görev yapan öğretim elemanları oluşturmaktadır. Çalışma basılı ve elektronik anket uygulaması ile 2013 Eylül ayı ile 2014 Mart ayı döneminde toplam 407 öğretim elemanına ulaşılarak gerçekleştirilmiştir. Araştırmaya katılan ve anketi geçerli olan 363 öğretim elemanının 20'si (%5,51) Prof.Dr., 40'ı (%11,02) Doç.Dr., 88'i (%24,24) Yrd.Doç.Dr., 16'sı (%4,41) Öğr.Grv.Dr, 63'ü (%17,36) Öğr.Grv., 9'u (%2,48) Arş.Grv.Dr., 99'u (%27,27) Arş.Grv., 1'i (%0,28) Okutman Dr., 5'i (%1,38) Okutman, 2'si (%0,55) Uzm.Dr., 10'u Uzm. unvanındadır. Araştırmaya katılan öğretim elemanlarının 175'i (%48,20) erkek ve 188'i (%51,80) kadındır. Araştırmaya katılan öğretim elemanlarının yaş aralığı 23 ile 65 arasında değişmekte olup yaş ortalaması ise 35,47'dir.

Veri Toplama Aracı. Çalışmayla ilgili uygulamanın ilk aşamasında alanyazın incelenerek bilgi güvenliği farkındalığı kavramına ilişkin göstergelerin neler olabileceği araştırılmıştır. Bilgi güvenliği farkındalığına ilişkin tespit edilmiş kategoriler, göstergeler ve madde sayıları Tablo 1'de sunulmuştur. Bilgi güvenliği farkındalığına ilişkin her bir gösterge göz önünde bulundurularak toplamda 90 maddelik bir havuz oluşturulmuştur.

Kapsam geçerliği çalışmalarında, Lawshe (1975) kapsam geçerliği tekniğinden yararlanılmıştır. Oluşturulan 90 maddelik deneme formu, Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE): 13, Bilgisayar Mühendisliği: 4, Bilgisayar Enformatik/ Bilgi Teknolojileri: 4, Elektronik Mühendisliği: 1 ve Bilişim Hukuku: 1 olmak üzere toplam 23 uzman tarafından değerlendirilmiştir. Her bir madde, bilgi güvenliği farkındalığını ölçebilme, ilgili alt boyutla ilişkili olma, ifadenin anlaşılırlığı başlıkları altında değerlendirilmiştir. Bu maksatla uzmanların herhangi bir maddeye ilişkin görüşleri toplanarak Kapsam Geçerlilik Oranları (KGO) elde edilmiştir. KGO'larının istatistiksel olarak anlamlılığı α=0,05 anlamlılık düzeyinde Veneziano ve Hooper (1997) tarafından tabloya dönüştüren kapsam geçerlik ölçütüyle (KGO20 = 0.42) karşılaştırılmış ve bu değerin altında kalan 23 madde çalışma kapsamından çıkartılmış (Keser ve Kavuk, 2015) ve bazı maddeler üzerinde düzeltmeler yapılmıştır. Çalışma sonucu oluşturulan 67 maddelik formun kapsam geçerlik indeksi 0.89 olarak hesaplanmıştır. Bireylerin, ölçekteki maddelere katılma düzeylerini belirlemek üzere "hiç katılmıyorum (1)", "katılmıyorum (2)", "kararsızım (3)", "katılıyorum (4)" ve "kesinlikle katılıyorum (5)" şeklinde Likert tipi beşli derecelendirme ölçeği kullanılmıştır.

Tablo 1. Bilgi Güvenliği Farkındalığı Kategori, Gösterge ve Madde Sayıları

Kategoriler	Göstergeler	Madde Sayısı
Genel Güvenlik	Bilgi güvenliği, Bilgi güvenliği sorumluğu, Anti-virüs yazılımları, Güvenlik duvarı, Şifre seçimi ve korunması, Virüs ve casus yazılımlar, Bazı yaygın söylenceler, İyi güvenlik alışkanlıkları, Çocukların güvenli şekilde çevrimiçi tutulması, Verilerin güvence altına alınması	34
Saldırı ve Tehditler	Çevrimiçi ticaret tuzakları, Sosyal mühendislik ve sazan avlama / yemleme saldırıları, Siber zorbalık, Aldatmacalar ve şehir efsaneleri, Kimlik hırsızlığı, Casus yazılımlar, Virüsler, solucanlar ve truva atları, Hizmet aksattırma saldırıları, Bozuk yazılım dosyaları, Kök kullanıcı takımı (rootkit) ve botnet'ler, Sahte anti-virüs yazılımları	21
E-posta ve İletişim	Anlık mesajlaşma ve sohbet odaları, Ücretsiz e-posta servislerinin faydaları ve riskleri, Mesaj sağanağı, Sosyal ağ siteleri, Dijital imza, E-posta istemcileri, E-posta ekleri	8
Mobil Cihazlar	Elektronik cihazlar için siber güvenlik, Cep telefonları ve kişisel dijital yardımcılar, Şahsi internet-etkin cihazlar ile seyahat, Taşınabilir cihazlarda veri güvenliği ve fiziksel güvenlik, Kablosuz ağ güvenliği, USB sürücüleri	8
Mahremiyet	Dosyaları n etkili bir şekilde silinmesi, Mahremiyetin korunması, Şifrelerin ilave önlemler ile desteklenmesi, Şifrelemenin anlaşılması	8
Güvenli Gezinme	Telif hakkı ihlalleri, Web sitesi sertifikaları, Web tarayıcıları, Aktif içerik ve çerezler, Web tarayıcılara ait güvenlik ayarları, Çevrimiçi güvenli alışveriş, Bluetooth teknolojisi, Uluslararası etki alan adları	6
Yazılım ve Uygulamalar	Son kullanıcı lisans sözleşmeleri, Dosya paylaşım teknolojileri ve riskler, Yazılım yamaları, Internet protokolü ses teknolojisi, İşletim sistemleri	5
Toplam		90

Verilerin Toplanması ve Analizi. Toplamda beş ay süren veri toplama süreci sonunda 407 öğretim elemanı, oluşturulan formun elektronik veya basılı halini doldurmuştur. Yapılan inceleme sonucunda öğretim elemanlarının doldurduğu 407 formdan 363'nün istatistiksel analize uygun olduğu tespit edilmiş, bu doğrultuda ölçeğin geçerlik ve güvenirlik çalışması yapılmıştır. Çakmak ve diğerleri (2014), ölçek geliştirme çalışmalarında ideal olan durumun Açımlayıcı Faktör Analizi (AFA) ve Doğrulayıcı Faktör Analizlerinin (DFA) farklı örneklem gruplarından elde edilen veriler üzerinde yapılması gerektiği şeklinde ifade etmektedir. Ancak, alanyazındaki ölçek geliştirme çalışmalarını inceleyen Çakmak ve diğerleri (2014) aynı örneklem grubunun rasgele alt gruplara bölünerek elde edilen veriler üzerinde de AFA ve DFA çalışmaları yapılabildiğini tespit etmişlerdir.

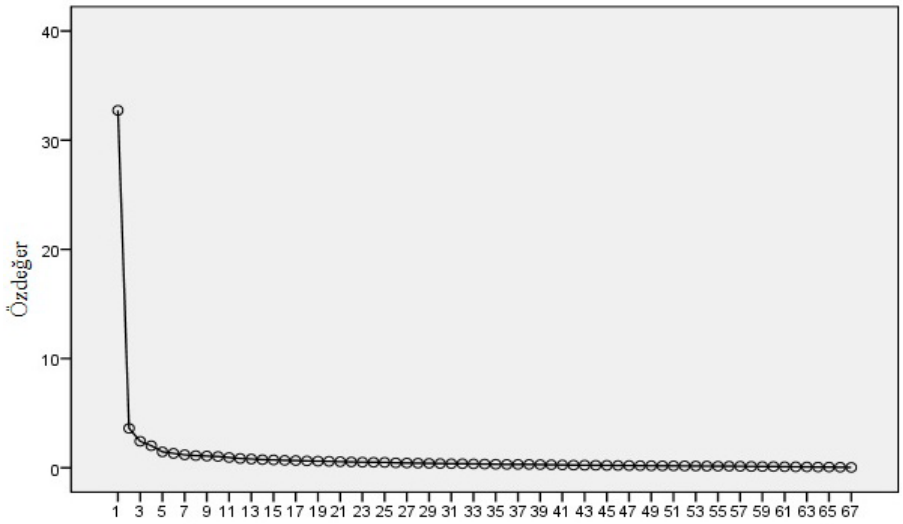
Örneklem büyüklüğü, madde ya da faktör sayısı gibi bağıl ölçütlere dayalı olarak tahmin edilmektedir. Genel olarak örneklem büyüklüğünün ölçekteki madde sayısının

5-10 katı kadar olması istenmektedir (Kass ve Tinsley, 1979; Kline, 1994; Tavşancıl, 2005). Kline (1994) mutlak ölçüt olarak 200 kişilik örneklemin yeterli olacağını, ancak büyük örneklemlerle çalışmanın daha uygun olacağını vurgulamaktadır. Çokluk, Şekercioğlu ve Büyüköztürk (2010), faktör analizinde en az 300 örneklem sayısının uygun olduğu genel kuralını ortaya koymaktadır. Bu çalışmada gerek zaman gerekse de maddi olanaklar göz önünde bulundurularak, araştırmaya katılan grup rasgele olarak iki alt gruba bölünmüştür (n1=363; n2=200). İlk grup üzerinde AFA, diğer grup üzerinde ise DFA yapılmıştır.

3. Bulgular ve Yorumlar

Verilerin AFA'ne uygunluğunu saptamak üzere Kaiser-Meyer-Olkin (KMO) Testi katsayısı hesaplanmış ve Barlett Küresellik testi yapılmıştır. Örneklem büyüklüğü için değer, 0.50'den düşük ise teste devam edilmez, .90 üzerinde ise "mükemmel" olduğu şeklinde yorumlanır (Tavşancıl, 2005; Çokluk ve ark., 2010). KMO katsayısı değeri .97 olarak belirlenmiştir ve veri yapısının faktör analizi yapabilmek için mükemmel derecede yeterli olduğu değerlendirmesi yapılabilir. Çalışma içerisinde yapılan analiz sonucunda Barlett Küresellik testi .01 düzeyinde manidar bulunmuştur [$\chi 2$= 23759.673; df=2211; p=0.000]. Bu bulgu, verilerin çok değişkenli normal dağılımdan geldiğini ve dolayısıyla faktör analizinin bir diğer sayıltısının karşılandığı anlamına gelmektedir.

Açımlayıcı Faktör Analizi. Faktör yapısını ortaya koymak için öncelikle döndürülmemiş temel bileşenler analizi gerçekleştirilmiştir. Faktör sayısının belirlenmesinde Kaiser-Guttman ilkesi uyarınca özdeğerleri 1'den büyük faktörlerin incelenmesi yoluna gidilmiş; faktör özdeğerlerine ilişkin çizgi grafiği ve açıkladıkları varyans oranları incelenmiştir (Zwick ve Velicer, 1986). Çünkü Faktör analizinde, sadece öz değerleri bir ve birin üzerinde olan faktörler kararlı olarak kabul edilir (Büyüköztürk, 2002; Çokluk ve ark., 2010). Ölçek, özdeğerleri 1'den büyük 10 faktör yapısına sahiptir. Bu faktörlerin sırasıyla özdeğeri ve açıklanan toplam varyansa katkı düzeyleri: 1.faktör:32,73; %48,85, 2.faktör: 3,61; %5,38, 3.faktör: 2,42; %3,62, 4.faktör: 2,02; %3,01, 5.faktör: 1,45; %2,17, 6.faktör: 1,32; %1,97, 7 faktör: 1,18; %1,77, 8.faktör: 1,11; %1,66, 9.faktör: 1,07; %1,60 ve 10.faktör: 1,03; %1,54 şeklindedir. Alanyazın incelendiğinde faktör yapılarına karar verebilmek için ortaya konulan çözümün kuramsal olarak temellenebilmesi olduğu görülmektedir (Zwick ve Velicer, 1986). Tek faktörlü desenlerde açıklanan varyansın %30 ve daha fazla olması yeterli görülebilir. Çok faktörlü desenlerde ise açıklanan varyansın daha yüksek olması beklenir. Açıklanan varyansı arttırmak için iki tür yol izlenir. Bunlardan ilki, önemli faktör sayısını arttırmak, ikincisi ise açıklanan madde seçiminde daha yüksek faktör yük değerini aramaktır (Büyüköztürk, 2002).



Bu kapsamda AFA analizine başlarken öz değer 2 ve faktör yük değeri 0.55 olarak kabul edilmiştir. Şekil 1'de faktör özdeğerlerine ait çizgi grafiği sunulmaktadır. AFA sonucunda ölçeğin öz değerinin 2'den büyük 4 faktör altında toplandığı görülmüştür. Bu 4 faktörün ölçeğe ilişkin açıkladığı varyans ise %60,86'dır. AFA sonucu oluşan maddeler binişiklik ve faktör yük değerlerinin kabul düzeyini karşılayıp karşılamaması açısından değerlendirilmiştir. Çok faktörlü desenlerde, binişik ve yük değeri düşük olan maddeler bir arada olabilir. Kesin bir kural olmamakla birlikte, madde çıkarma işlemine binişik maddelerden başlanması tercih edilebilir (Çokluk ve ark., 2010). Binişik ve yük değeri düşük olan maddeler ölçekten çıkartılarak AFA 34 kez tekrarlanmıştır. Nihai AFA sonucu oluşan, maddelere ilişkin faktör yükleri ve ortak faktör varyansı Tablo 2'de sunulmuştur.

Şekil 1. Faktör Özdeğerlerine İlişkin Çizgi Grafiği

Tablo 3 incelendiğinde ölçekte yer alan 16 maddeden oluşan birinci faktöre ait faktör yük değerlerinin .62 ile .88 arasında, maddelere ilişkin ortak faktör varyanslarının ise .57 ile .81 arasında değiştiği; 18 maddeden oluşan ikinci faktör ait faktör yük değerlerinin .58 ile .74 arasında, maddelere ilişkin ortak faktör varyanslarının ise .43 ile .57 arasında değiştiği görülmektedir. Toplam varyansa en yüksek katkıyı.88 faktör yük değeri ve .81 ortak faktör varyansı ile 33. maddenin, en düşük katkıyı ise .58 faktör yük değeri ve .43 ortak faktör varyansı ile 62. maddenin yapmakta olduğu ifade edilebilir. Birinci faktörün açıklayabildiği toplam varyans %31,97 düzeyinde olup, alanyazın da dikkate alınarak "saldırı ve tehditler" olarak isimlendirilmiştir. İkinci faktörün açıklayabildiği varyans %28,59 düzeyinde olup, alanyazın da dikkate alınarak "kişisel verilerin korunması" olarak isimlendirilmiştir.

Tablo 2. Faktör Yük Değerleri ve Ortak Faktör Varyansı

Alt Boyut	Madde	F1	Ortak Faktör Varyansı	Alt Boyut	Madde	F2	Ortak Faktör Varyansı
Saldırı ve Tehditler	S33	0,88	0,81	*Kişisel Verilerin Korunması*	S41	0,74	0,57
	S32	0,87	0,79		S44	0,74	0,62
	S30	0,84	0,76		S46	0,72	0,64
	S31	0,81	0,76		S45	0,72	0,61
	S36	0,79	0,73		S61	0,70	0,65
	S22	0,79	0,67		S42	0,68	0,58
	S35	0,78	0,73		S43	0,68	0,64
	S34	0,78	0,70		S39	0,67	0,47
	S28	0,76	0,73		S38	0,67	0,52
	S26	0,75	0,71		S8	0,66	0,53
	S20	0,72	0,66		S9	0,63	0,47
	S29	0,71	0,66		S6	0,61	0,47
	S25	0,71	0,68		S51	0,60	0,46
	S21	0,67	0,69		S1	0,59	0,40
	S27	0,65	0,64		S10	0,59	0,40
	S23	0,62	0,57		S40	0,58	0,46
					S2	0,58	0,43
					S62	0,58	0,43
	Özdeğer:		17,74		Özdeğer:		2,85
	Açıklanan Varyans:		31,97		Açıklanan Varyans:		28,59
					Açıklanan Toplam Varyans:		60,57

İki faktörlü yapının açıklayabildiği toplam varyans %60,57 düzeyindedir. Alanyazında çok faktörlü ölçek yapılarında, sosyal bilimlerde açıklanan varyansın %40 ile %60 arasında olması yeterli olarak kabul edilir (Tavşancıl, 2005). Bu ölçüte dayanarak elde edilen iki faktörlü ölçek yapısı öğretim elemanlarına yönelik bilgi güvenliği farkındalığını ölçmek için yeterli bulunmuştur. Ölçekte yer alan otuz dört maddenin tamamı için faktör yük değerleri .58'in üzerinde kalmıştır. Alanyazında .45 ve üzerinde faktör yük değeri gösteren maddeler ölçekte kesinlikle tutulması gereken maddeler olarak nitelenmektedir (Büyüköztürk, 2011: 124; Kline, 2000: 167-168). Bu ölçüte dayanarak ölçeğin iki faktör altında otuz dört maddenin tamamını içermesine karar verilmiştir.

Madde Analizleri. Ölçekte yer alan her bir maddenin, ölçmek istediği özelliği ölçüp ölçmediği ve ölçtükleri özellik açısından kişileri ayırt etmede ne kadar yeterli olduklarının belirlenmesi amacıyla ilk olarak madde-toplam korelasyonları hesaplanmıştır. İkinci olarak ise toplam puana göre üst %27 ve alt %27'lik grupların madde

puanları arasındaki farkın anlamlılığı için t-testi kullanılmıştır. Ayrıca, ölçeğin güvenirliğini belirlemek için Cronbach alfa iç tutarlılık katsayısına bakılmıştır. Ölçekte yer alan her bir madde için madde-toplam korelasyonları ve toplam puana göre belirlenen üst ve alt %27'lik grupların madde puanları arasındaki farkın anlamlılığını irdeleyen bağımsız t-testi sonuçları Tablo 3'te sunulmaktadır.

Tablo 3. Madde Analiz Sonuçları

F1	Madde	Düzeltilmiş Madde-Toplam Korelasyonu	Üst-Alt %27 Farkın Anlamlılık Testi (Bağımsız t-testi)	F2	Madde	Düzeltilmiş Madde-Toplam Korelasyonu	Üst-Alt %27 Farkın Anlamlılık Testi (Bağımsız t-testi)
Saldırı ve Tehditler	S20	0,79	21,75*	Kişisel Verilerin Korunması	S01	0,59	10,04*
	S21	0,80	22,40*		S02	0,62	11,32*
	S22	0,79	16,64*		S06	0,64	12,56*
	S23	0,72	16,92*		S08	0,69	12,30*
	S25	0,80	22,26*		S09	0,65	11,79*
	S26	0,83	23,04*		S10	0,58	10,12*
	S27	0,76	17,92*		S38	0,68	12,33*
	S28	0,83	21,05*		S39	0,61	9,18*
	S29	0,78	20,57*		S40	0,63	13,02*
	S30	0,83	18,43*		S41	0,68	11,34*
	S31	0,85	20,52*		S42	0,72	15,88*
	S32	0,84	17,39*		S43	0,76	17,15*
	S33	0,84	16,57*		S44	0,75	13,04*
	S34	0,81	20,00*		S45	0,74	14,28*
	S35	0,82	20,48*		S46	0,77	16,57*
	S36	0,83	19,97*		S51	0,63	10,18*
					S61	0,77	16,17*
					S62	0,61	12,61*

Faktör analizi ile belirlenen iki boyutu oluşturan 34 maddenin madde analizleri yapılmıştır. Buna göre; saldırı ve tehditler faktöründe madde-toplam test korelasyonları incelendiğinde değerler r=.72 ile r=.85 arasında değişmektedir. Kişisel verilerin korunması faktöründe madde-toplam test korelasyonları incelendiğinde değerler r=.59 ile r=.77 arasında değişim göstermektedir. Madde- toplam korelasyonlarının .30 ve daha yüksek olması ölçek maddelerinin geçerliğine bir kanıt olarak kullanılmaktadır (Nunnally ve Bernstein, 1994). Madde-toplam test korelasyonları incelendiğinde, her bir madde için (r=.30)'un üzerindedir. Bu durum, ölçek maddelerinin ölçülmek istenen özelliği ölçme amacına hizmet ettiğine işaret etmektedir. Ayrıca, ölçeğin t-testi

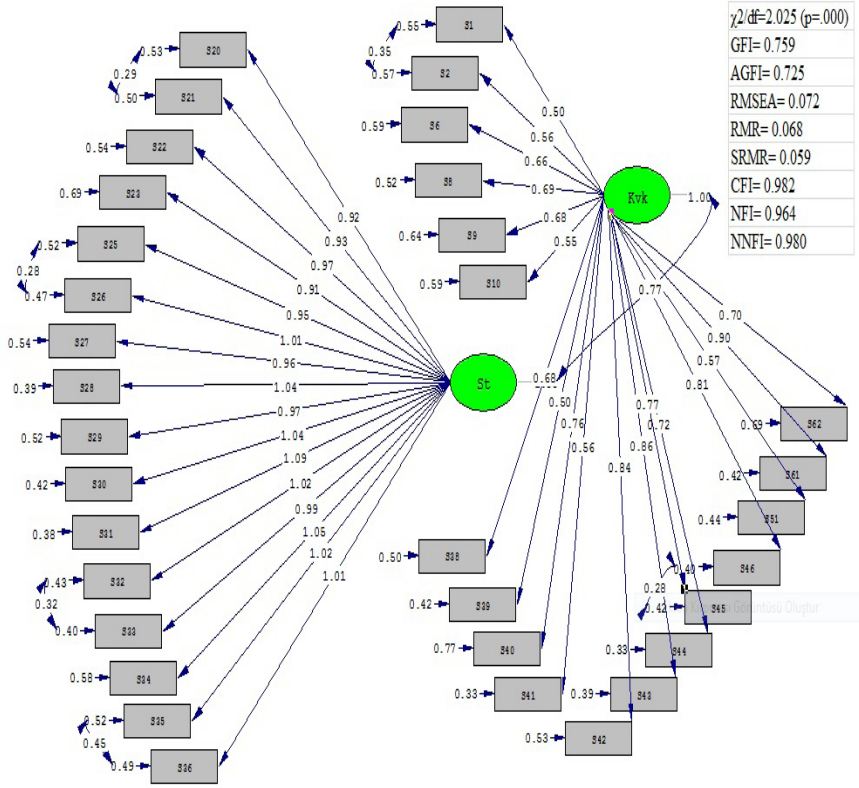
sonuçlarına göre %27 alt ve üst gruplarının madde puanları arasındaki farklara ilişkin t testi değerlerinin 9.18-23.04 arasında değiştiği ve hepsinin de anlamlı olduğu ($p<$ .001) görülmektedir. Üst %27'lik grubun tüm maddelere ilişkin madde puan ortalamaları alt %27'lik grubun madde puan ortalamalarından anlamlı biçimde yüksektir. Buna göre ölçekte yer alan maddeler aynı davranışı; yani öğretim elemanlarına yönelik bilgi güvenliği farkındalığını ölçmekte ve farklı farkındalık seviyelerindeki katılımcıları anlamlı biçimde ayırt edebilmektedir. Hem madde-toplam korelâsyonları hem de üst ve alt %27'lik grupların madde ortalama puanlarına ilişkin t-testi sonuçları ayırt ediciliği en yüksek olarak 33. ve en düşük olarak 62. maddeyi göstermektedir.

Ölçeğin güvenirliğini ortaya koymak amacıyla Cronbach Alfa iç tutarlılık katsayısı hesaplanmıştır. Genel olarak, güvenilirlik katsayılarının .70 veya daha yüksek olması, yeterli olarak değerlendirilmektedir (Nunnally, 1978). Ölçeğin tümüne ait Cronbach alfa iç tutarlılık katsayısı .97, birinci alt faktöre ilişkin Cronbach alfa iç tutarlılık katsayısı .97, ikinci alt faktöre ilişkin Cronbach alfa iç tutarlılık katsayısı .94 olarak hesaplanmıştır. Tüm bu bulgular ölçeğin tatmin edici düzeyde güvenirliğe sahip olduğunu göstermektedir. Bunun yanında madde-toplam korelasyonlarının yüksekliği de ölçeğin iç tutarlılığının gücüne işaret etmektedir.

Doğrulayıcı Faktör Analizi. AFA sonrasında ortaya çıkan modelin, yapı geçerliğini değerlendirmek için DFA yapılmıştır (Kline, 2005). Bu çalışmada model uyum indeksleri olarak Ki-Kare ($\chi 2$) İyilik Uyumu, İyilik uyum İndeksi (GFI), Düzenlenmiş İyilik Uyum İndeksi (AGFI), Yaklaşık Hataların Ortalama Karekökü (RMSEA), Artık Ortalamaların Karekökü (RMR), Standardize Edilmiş Artık Ortalamaların Karekökü (SRMR), Karşılaştırmalı Uyum İndeksi (CFI), Normlaştırılmış Uyum İndeksi (NFI) ve Normlaştırılmamış Uyum İndeksi (NNFI) göz önünde bulundurulmuştur.

İki faktörden oluşan yapıya ilişkin olarak gerçekleştirilen doğrulayıcı faktör analizlerinde model üzerinde hiçbir sınama yapılmadan ve önerilen modifikasyonlar gerçekleştirilmeden önce ulaşılan uyum iyiliği indeksleri şöyledir: [$\chi 2/df=3.587$ ($p=.000$); GFI= 0.630; AGFI= 0.581; RMSEA= 0.114; RMR= 0.077; SRMR= 0.066; CFI= 0.953; NFI= 0.936; NNFI= 0.950]. Analizler sonucunda ortaya çıkan modifikasyon önerileri incelendiğinde; S36 ve S35; S33 ve S32; S46 ve S45; S2 ve S1; S21 ve S20; S26 ve S25 maddeleri arasında altı modifikasyon önerisinin ortaya çıktığı görülmüştür.

Kuramsal olarak incelendiğinde; bu maddelerin benzer durumları ölçtükleri, dolayısıyla iki madde arasında gizil bir ilişkinin kabul edilebilir olacağı görülmüş ve modifikasyon önerisi dikkate alınmıştır.



Şekil 2. Doğrulayıcı Faktör Analizi

Modifikasyonun ardından modele ilişkin uyum iyiliği indeksleri şu şekilde oluşmuştur: [χ2/df=2.025 (p=.000); GFI= 0.759; AGFI= 0.725; RMSEA= 0.072; RMR= 0.068; SRMR= 0.059; CFI= 0.982; NFI= 0.964; NNFI= 0.980]. Şekil 2'de iki faktörlü yapıya ilişkin yapısal eşitlik modeli ve Tablo 4'te ölçek maddelerine ilişkin t ve R2 (çoklu korelasyon katsayısı) değerleri sunulmaktadır.

Tablo halinde sunulan yapısal eşitlik modelinde uyum indeksleri kriterleri ve kabulü için kesme noktaları göz önüne alınarak modelin uyum iyiliği indeksleri incelendiğinde Ki-Kare/serbestlik derecesi iyilik uyumu değerinin 2.025 olduğu görülmektedir (küçük örneklemler için 2.5'in altındaki modellerde mükemmel uyum, Çokluk ve arkadaşları, 2010; Kline, 2005). Hesaplanan RMSEA değerinin .07 olduğu görülmektedir (iyi uyum, Brown, 2006; Jöreskog ve Sörbom, 1993). Modelin GFI değeri .76 ve AGFI değeri .73 için zayıf uyuma sahip olduğu söylenebilir (GFI, AGFI > .90 mükemmel uyum; GFI> .85 ve AGFI>.80 kabul edilebilir uyum; Jöreskog ve Sörbom, 1993). Alanyazın irdelendiğinde bu indekslerin aldıkları değerlerin örneklem büyüklüğünden etkilenebildikleri görülmektedir (Şimşek, 2007:

48). Örneklem büyüklüğü etkilerinden arındırılmış uyum iyiliği indekslerinden olan CF, NFI ve NNFI üzerinde durulmuştur. CFI, NFI ve NNFI değerlerinin .95'den büyük olduğu görülmektedir (CFI, NFI, NNFI > .95 mükemmel uyum; Sümer, 2000; Thompson, 2004). RMR ve SRMR değerinin .08'den küçük olması iyi uyuma sahip olduğunu göstermektedir (Brown, 2006; Byrne, 1994). Modele ilişkin t değerleri incelendiğinde tüm gözlenen değişkenlerin gizil değişken tarafından .01'lik anlamlılık düzeyinde yordanabildiği görülmektedir.

Tablo 4. Maddelere İlişkin t ve R^2 Değerleri

F1	Madde	t	R^2	F2	Madde	t	R^2
Saldırı ve Tehditler	S31	15,50	0,76	*Kişisel Verilerin Korunması*	S27	13,46	0,63
	S28	15,15	0,74		S46	13,23	0,62
	S30	14,91	0,72		S20	13,16	0,61
	S33	14,74	0,71		S44	13,07	0,61
	S32	14,72	0,71		S45	12,63	0,58
	S26	14,31	0,68		S42	12,49	0,57
	S36	14,12	0,67		S23	12,15	0,55
	S35	14,08	0,67		S41	11,09	0,48
	S61	13,86	0,66		S08	11,05	0,48
	S34	13,85	0,66		S38	11,04	0,48
	S43	13,73	0,65		S40	10,29	0,43
	S29	13,70	0,65		S51	10,21	0,43
	S02	9,10	0,65		S06	10,18	0,42
	S22	13,60	0,64		S09	10,10	0,42
	S25	13,52	0,64		S62	10,06	0,42
	S21	13,51	0,63		S39	9,43	0,38
					S10	8,90	0,34
					S01	8,46	0,31

Önemli bir ölçüt de her bir gözlenen değişken için açıklanan varyansı ifade ederek, gözlenen değişkenin gizil değişkendeki değişimin ne kadarını açıklayabildiğini ortaya koyan R^2 değeridir (Şimşek, 2007: 86). Modele ilişkin λx, t ve R^2 değerleri incelendiğinde bilgi güvenliği farkındalığının ölçümüne en yüksek katkıyı sırasıyla 31, 28, 30, 33 ve 32. maddelerin, en düşük katkıyı ise sırasıyla 1, 10, 39, 62, 9. maddelerin sağladığı görülmektedir. Bu bulgu, açımlayıcı faktör analizinde elde edilen bulguları doğrulamaktadır.

4. Tartışma

Alanyazın incelemesinde bilgi güvenliği konusunda yapılan çalışmaların bilgi güvenliği ile bilgi güvenliği yönetim sistemlerine yönelik olduğu ve bu bağlamda "en zayıf halka" olan insan unsurunu bilgi güvenliği konusunda bilinçlendirme üzerinde durulduğu tespit edilmiştir. Bu çalışmalarda, bilgi güvenliği farkındalığına yönelik çeşitli tavsiyeler ve alınması gereken tedbirler sunulmaktadır. Ayrıca ulaşılan kaynaklar kapsamında, kullanıcıların mevcut farkındalık düzeylerini belirleyebilecek tek çalışmanın yurtdışı kaynaklı olduğu, yurt içinde ise bu konuda bir çalışmaya yer verilmediği tespit edilmiştir. Bu araştırma kapsamında alanyazından elde edilen bilgi güvenliği farkındalık göstergeleri esas alınarak yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerini belirleyecek yeni bir ölçek geliştirilmiştir.

Yapı geçerliliği çalışmalarında ölçekte yer alan 34 madde 2 faktör altında toplanmış ve açıklayabildiği toplam varyans %60,57'dir. Bu oran çok faktörlü ölçek yapısı için yeterli kabul edilmektedir. İlk faktör 'saldırı ve tehditler' olarak isimlendirilmiş ve açıklayabildiği toplam varyans %31,97'dir. İkinci faktör 'kişisel verilerin korunması' olarak isimlendirilmiş ve açıklayabildiği toplam varyans %28,59'dur. Madde analizlerinde, madde toplam puanları arasında güçlü bir korelasyonel ilişki belirlenmiştir. Ölçeğin tamamına ait Cronbach alfa iç tutarlılık katsayısı .97, alt faktörlere ilişkin değerler .97 ve .94 olarak hesaplanmıştır. Madde toplam korelâsyonları ve iç tutarlılık katsayıları dikkate alındığında geliştirilen ölçeğin güvenilir olduğu düşünülmektedir.

Doğrulayıcı faktör analizinin ortaya koyduğu uyum iyiliği indeksleri ve standart değerler açımlayıcı faktör analiziyle ortaya konan çok faktörlü yapının uygunluğuna işaret etmektedir. Özellikle X^2/df, CFI, NFI ve NNFI değerleri göz önüne alındığında yapının mükemmel uyuma sahip olduğunu ortaya koymaktadır. RMSEA, RMR ve SRMR değerleri göz önüne alındığında iyi uyuma sahip olduğunu ortaya koymaktadır. GFI, AGFI değerleri göz önüne alındığında, yakın olmakla birlikte kabul edilebilirlik sınırlarının dışında değer göstermektedirler. Bu noktada bir sınırlılık olarak araştırmada kullanılan örneklemin AFA ve DFA aynı anda kullanılmasından kaynaklandığı söylenebilir. Dolayısıyla doğrulayıcı faktör analizinde kabul edilebilirlik sınırı altında değer gösteren indekslerin araştırma grubunun sınırlılığından etkilenmiş olabilecekleri düşünülmektedir.

Araştırmadaki diğer bir sınırlılık öğretim elemanlarının bu tür çalışmalara katılmada gönülsüz olmalarıdır. Bu duruma ölçek geliştirme esnasında araştırma grubunu oluşturan öğretim elemanlarının iş yoğunluğu ve araştırma konusuna yeterli zaman ayıramamalarının sebep olduğu düşünülmektedir. Geliştirilen ölçeğe ilişkin faktör yük değerleri, iç tutarlılık katsayıları gibi istatistiksel parametrelerdeki birtakım değişimlerde bu isteksizliğin de etkili olabileceği düşünülmektedir. Ayrıca çalışma grubunun büyüklüğü açımlayıcı faktör analiziyle elde edilen değerleri de etkileyebilecek bir sınırlılık olarak ele alınabilir. Gelecekte daha geniş katılımcı

grupları üzerinde ölçeğin faktör yapısının yeniden sorgulanmasının yararlı olacağı düşünülmektedir.

Bu çalışma sonucu ölçeğin psikometrik özellikleri, geçerli ve güvenilir bir yapıda olduğunu göstermektedir. Bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik çalışmalarda, kişilerin farkındalık düzeyleri, geliştirilen ölçek aracılığıyla belirlenebilir. Belirlenen farkındalık düzeyleri, geliştirecek eğitim yardımcı materyalleri ile kişilerin bilinmeyen ya da az bilinen konulardaki farkındalıkları geliştirilebilir. Ayrıca, geliştirilen ölçeğe ilişkin geçerlik ve güvenirlik çalışmaları zaman ve maddi imkânlar göz önünde bulundurularak aynı örneklem grubu üzerinde gerçekleştirilmiştir. Gelecek çalışmalarda farklı örneklem grubu üzerinde geliştirilen ölçeğin geçerlik ve güvenirlik değerleri test edilebilir.

5. Kaynakça

Acılar, A. (2009). İşletmelerde Bilgi Güvenliği ve Örgüt Kültürü. *Organizasyon ve Yönetim Bilimleri Dergisi, I*(1), 25-33.

Brown, T. A. (2006). Confirmatory factor analysis for applied research. New York: Guilford.

Byrne, B. M. (1994). Structural equation modeling with EQS and EQS/Windows: Basic concepts, applications, and programming. Thousand Oaks, CA: Sage.

Büyüköztürk, Ş. (2002). Faktör Analizi: Temel Kavramlar ve Ölçek Geliştirmede Kullanımı. Kuram ve Uygulamada Eğitim Yönetimi. Cilt 32, 470-483.

Büyüköztürk, Ş. (2011). Sosyal bilimler için veri analizi el kitabı. Ankara: Pegem Akademi Yayıncılık.

Caruso, J. B. (2003). Information Technology Security: Governance, Strategy, and Practice in Higher Education. Wisconsin, Madison: EDUCAUSE Center For Applied Research ECAR. Retrieved from http://net.educause.edu/ir/library/pdf/EKF/ekf0305.pdf

Chen, C. C., Shaw, R., and Yang, S. C. (2006). Mitigating Information Security Risks By Increasing User Security Awareness: A Case Study Of An Information Security Awareness System. Information Technology, Learning and Performance Journal, 24(1), 1-14.

Çakmak, E.Kılıç, Çebi, A. ve Kan, A. (2014). E-öğrenme Ortamlarına Yönelik"Sosyal Bulunuşluk Ölçeği" Geliştirme Çalışması. Kuram ve Uygulamada Eğitim Bilimleri, 14(2), 755-768.

Çokluk, Ö., Şekercioğlu, G. ve Büyüköztürk, Ş. (2010). Sosyal bilimler için çok değişkenli istatistik SPSS ve LISREL uygulamaları. Ankara: Pegem Akademi.

Cox, A., Connolly, S., and Currall, J. (2001). Raising Information Security Awareness In The Academic Setting, VINE, Vol.31 Iss:2, pp.11-16, Glasgow, United Kingdom. doi: 10.1108/03055720010803961

Foster, A. L. (2004). Insecure and Unaware. Chronicle of Higher Education, 50(35), 33-35.

Gülmüş, M. (2010). Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği. (Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Elektrik Mühendisliği Anabilim Dalı, İstanbul). http://tez2.yok.gov.tr/ adresinden edinilmiştir.

Jöreskog, K. G., and Sörbom, D. (1993). LISREL 8: Structural equation modeling with the SIMPLIS command language. Chicago: SSI Scientific Software International Inc.

Kass, R. A., and Tinsley, H. E. A. (1979). Factor analysis. Journal of Leisure Research, 11, 120-138.

Keser, H. ve Kavuk, M. (2015). Okulda siber zorbalık farkındalık anketinin geliştirilmesi. *Kastamonu Eğitim Dergisi,* 23(1), 17-30.

Kjorvik, H. (2010). Implementing and improving awareness in information security. (Master's thesis, University of Agder, Faculty of Engineering and Science, Grimstad). Retrieved from http://brage.bibsys.no/

Kline, P. (1994). An easy guide to factor analysis. New York: Routledge.

Kline, P. (2000). The Handbook of Psychological Testing (2nd Edition). London and New-york: Routledge.

Kritzinger, E., and Smith, E. (2008). Information security management:An information security retrieval and awareness model for industry. Computer and Security, 27, 224-231.

Kruger, H., and Kearney, W. D. (2006). A prototype for assessing information security awareness. Computer and Security, 25, 289-296.

Lawshe, C. H. (1975). Aquantitative approach to content validity. Personnel Psychology, 28, 563–575.

Mahabi, V. (2010). Information security awareness: System administrators and end-user perspectives at Florida State University.(Doctoral dissertation, The Florida State University, College of Communication and Information, Florida). Retrieved from http://diginole.lib.fsu.edu/etd/2798/

Mathisen, J. (2004). Measuring information security awareness - A survey showing the Norwegian way to do it.(Master's thesis, Gjovik University, College Institutionen for Data- och Systemvetenskap, Hogskolen). Retrieved from http://brage.bibsys.no/

Nunnally, J. C. (1978). Psychometric testing. New York: McGraw-Hill.

Nunnally, J. C., and Bernstein, I. (1994). Psychometric theory. New York: McGraw-Hill.

Özcan, B. (2009). Kurumsal bilgi güvenliği ve COBIT. (Yüksek lisans tezi, Haliç Üniversitesi, Yönetim Bilişim Sistemleri Anabilim Dalı, İstanbul). http://tez2.yok.gov.tr/ adresinden edinilmiştir.

Penmetsa, M. K. (2010). A methodology for measuring information security maturity in Norwegian and Indian MSME's with special focus on people factor. (Master's thesis, Gjovik University, College Department of Computer Science and Media Technology, Hogskolen). Retrieved from http://brage.bibsys.no/

Puhakainen, P. (2006). A Design theory for information security awareness. (Master's thesis, Acta University of Oulu, Faculty of Science Department of Information Processing Science, Oulu). Retrieved from http://herkules.oulu.fi

Rezgui, Y., and Marks, A. (2008). Information security awareness in higher education: An exploratory study. Computer and Security, 27, 241-253.

Siponen, M. T. (2001, June). Five Dimensions Of Information Security Awareness. Computer and Society, s. 24-29.

Sümer, N. (2000). Yapısal eşitlik modelleri: Temel kavramlar ve örnek uygulamalar. Türk Psikoloji Yazıları, 3(6), 49-74.

Şahinaslan, E., Kandemir, R. ve Şahinaslan, Ö. (2009). Bilgi Güvenliği Farkındalık Eğitimi Örneği. Akademik Bilişim ‹09 - XI.Akademik Bilişim Konferansı Bildirileri, (s. 189-194). Urfa.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri. Akademik Bilişim ‹09 - XI.Akademik Bilişim Konferansı Bildirileri, (s. 597-602). Şanlıurfa.

Şimşek, Ö. F. (2007). Yapısal Eşitlik Modellemesine GirişTemel İlkeler ve LISREL Uygulamaları. Ankara: Ekinox.

Tabachnick, B.G. and Fidel, L.S. (2001). Using multivariate statistics. MA: Allyn and Bacon, Inc.

Tavşancıl, E. (2005). Tutumların ölçülmesi ve SPSS ile veri analizi. Ankara: Nobel.

Thompson, B. (2004). Exploratory and confirmatory factor analysis: Understanding concepts and applications. Washington, DC: American Psychological Association.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. Information Security Journal: A Global Perspective, 207-227.

Vardal, N. (2009). Yükseköğretimde bilgi güvenliği: Bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması. (Doktora Tezi, Gazi Üniversitesi, Eğitim Bilimleri Ana Bilim Dalı, Ankara). http://tez2.yok.gov.tr/ adresinden edinilmiştir.

Veiga, A. d. (2008). Cultivating and assessing information security culture. (Doctoral dissertation, University of Pretoria, Faculty of Engineering, Built Environment and Information Technology, Pretoria). Retrieved from http://upetd.up.ac.za/thesis/available/etd-04242009-165716/

Veneziano L. ve Hooper J. (1997). Amethod for quantifying content validity of health-related questionnaires. American Journal of Health Behavior, 21(1):67-70.

Vural, Y. (2007). Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri. (Yüksek lisans tezi, Gazi Üniversitesi, Bilgisayar Mühendisliği Anabilim Dalı, Ankara). http://tez2.yok.gov.tr/ adresinden edinilmiştir.

Vural, Y. ve Sağıroğlu, Ş. (2011). Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler. Mühendislik Mimarlık Fakültesi Dergisi, 26(1), 89-103.

Zwick, W. R., & Velicer, W. F. (1986). Comprasion of five rules for determining the number ofcomponents to retain. Psychological Bulletin, 99(3),432-442.

EXTENDED ABSTRACT

Information has been one of the most important factors in the life of human beings. Mankind has been sought after to reach, have and make use of information to have a better life. This necessity has been the most important reason for the rapid development of information and communications technologies. With the development of information and communications technology, limitations caused by factors such as time, space and geographical distance have

disappeared. Many tasks and operations being carried out in daily life has become easy and can be done quickly. For instance, obtaining information from various resources such as government agencies, banks, hospitals, etc., or performing many different tasks such as making reservations, buying tickets, finding test results, registering events, are among the first that come to mind.

Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Confidentiality, integrity and availability are sometimes referred to as the CIA triad of information security. In case of the three basic security elements is damaged, then security weakness occurs. The spread of information and communications technologies as well as the use of the Internet and the increase in online applications widely used on the Internet lead to amplified vulnerability. So it is everyone's own responsibility to ensure the security of information in society. However, most IS security managers attach attention merely to technical solutions such as firewalls, routers, and intrusion detection software, while pay less focus on soft issues such as the hazards caused by end users' lack of IS security awareness. IS security awareness plays a significant role in the process of the overall information security of any organization. Humans might be the weakest link in the chain of security control. Thus, one effective preventive measure is to create a security-aware culture by educating all staff about security risks and their responsibilities.

Universities are working more and more online like many other institutions. The more institutions depend on computers, the more important computer security becomes. The risks are serious in the academic sector as in the other sectors such as defense, finance etc. For institutions, security failures cause a waste of time, data and reputation. The individuals have similar things at stake along with their privacy. The number of scientific studies that consider IS security awareness especially in higher education environments is very limited. Creating information security awareness is a dynamic process due to continuously changing risk, which makes it even more difficult. As a result, any awareness program needs to be continually measured and managed to keep abreast of changes in risk profiles.

Thus, the purpose of this study is to develop an "information security awareness scale" for faculty members to determine the level of information security awareness. A systematic approach is followed for developing the scale. After the review of a wide range of literature, the indicators on the concept of information security awareness has been investigated. Published studies are categorized as general security, attacks and threats, email and communication, mobile devices, privacy, secure browsing, software and applications. The study was conducted with 363 faculty members working in various higher education institutions in Turkey using printed and electronic surveys. The sample is split into two subsamples on a random basis (n1=363; n2=200). The first sample is used for Exploratory Factor Analysis and the second sample for Confirmatory Factor Analysis. As a result of exploratory factor analysis, it was determined that the scale consists of 34 items and 2 subscales ('attacks and threats' and 'the protection of personal data'). Confirmatory factor analysis was conducted with randomly selected group of 200 academicians among participants. Two-factor structure was confirmed [$\chi 2/df=2.025$ ($p=.000$); GFI=.759; AGFI=.725; RMSEA=.072; RMR=.068; SRMR=.059; CFI= .982; NFI=.964; NNFI=.980]. Cronbach's alpha reliability coefficient is .97 for the entire scale; .94, .97, respectively, for each subscale. Consequently in this study, a valid and reliable instrument that can be used to determine the level of information security awareness of faculty members has been developed.

This study has some limitations about sampling. The first important limitation of this study is that the sample is split into two subsamples on a random basis for AFA and CFA. The other limitation of this study is the fact that faculty members are reluctant to participate in such studies. This is because of the height of the working pace of the faculty members and are not allocated adequate to research. In the future a wider group of participants are considered to be beneficial questioned again on the factor structure of the scale.