ATLAS INTERNATIONAL REFEREED JOURNAL ON SOCIAL SCIENCES
ISSN:2619-936X
Article Arrival Date:01.10.2018 | Published Date:30.11.2018
2018 / November | Vol 4, Issue:14 | Pp:1522-1543
Disciplines: Areas of Social Studies Sciences (Economics and Administration, Tourism and Tourism Management, History, Culture, Religion, Psychology, Sociology, Fine Arts, Engineering, Architecture, Language, Literature, Educational Sciences, Pedagogy & Other Disciplines in Social Sciences)

İBER RİSKLER KARŞISINDA KOBİ'LERİN BİLGİ GÜVENLİĞİ FARKINDALIĞINI ÖLÇEN BİR ÖLÇEK GELİŞTİRME: GAZİANTEP ÖRNEKLEMİ

A SCALE DEVELOPMENT ABOUT INFORMATION SECURITY AWARENESS OF SMES AGAINST CYBER RISKS: SAMPLE OF GAZIANTEP

Dr. Cüneyt ÇATUK

cuneytcatuk@hotmail.com, Gaziantep/Turkiye

Prof.Dr. Gülçimen YURTSEVER

Hasan Kalyoncu Üniversitesi Gaziantep/Türkiye

ÖZET

Globalleşen dünya ve İnternet teknolojisinin sağladığı avantajlardan sonra KOBİ'ler bölgesel şirketler olmaktan çıkıp global firmalar haline geldiler. İnternetin ve globalleşmenin sağladığı bu avantajın yanında KOBİ'ler için, bazı risklerin oluşmasına neden oldu. Bu nedenle, bu çalışma KOBİ'lerin bilgi güvenliği farkındalıklarını ölçmek için bir ölçek geliştirilmesi amacıyla yürütülmüştür.

Bu ölçeğin İçerik/Kapsam geçerliği, Ölçüt-Bağlımlı Geçerliliği ve Yapı Gerçerliliği ispatlanmıştır. İç tutarlık Güvenirliği için Cronbach alfa katsayısı kullanılmıştır. Keşfedici ve Doğrulayıcı Faktör analizi yapılmıştır.

Ölçekte 37 madde bulunmaktadır. Veriler Gaziantep'te farklı sektörlerde faaliyet gösteren 800 KOBİ çalışanın anket sorularına verdikleri cevaplardan elde edilmiştir. Araştırma sonuçlarına göre bu ölçeğin dört alt boyutu vardır. Dört alt boyutun toplam varyansın %67,33'ünü açıklamıştır.

Çalışmanın önemi KOBİ çalışanlarının çalıştıkları firmalarda bilgi güvenliği ile ilgili farkındalığın algılanmasını ölçmeye yönelik yeni, geçerli ve güvenirliği olan bir ölçek olmasıdır. Bu ölçek KOBİ'lerin bilgi güvenliği ile ilgili üzerinde durulması gereken hususlara yardımcı olabilir.

Anahtar sözcükler: Farkındalık, Bilgi Güvenliği, KOBİ, Ölçek

ABSTRACT

After the advantages provided by the globalizing world and Internet technology, the Small and Medium Enterprises(SMEs) have become global companies from being regional companies. In addition to this advantage provided by the Internet and globalization, it also caused some risks for SMEs. For this reason, this study was conducted to develop a scale to measure the awareness of information security of SMEs.

Content / Scope validity, criterion / related validity and construct validity of this scale have been proven. Exploratory factor analysis and confirmatory factor analysis were utilized for the construct validity, and Cronbach's alpha coefficient was used for internal consistency reliability.

There are 37 items on the scale. The data were obtained from the answers of 800 SMEs employees working in different sectors in Gaziantep to the questionnaire survey. According to the results of the research, this scale has four sub dimensions. Four sub-dimensions explain 67.33% of the total variance.

The importance of the study constucted a new, valid and reliable scale to measure the perception of information security awareness in firms where SMEs employees are working. The result of this study may help to develop a better understanding of where SMEs need to focus information security concerns.

Key words: Awareness, Information Securities, SMEs, Scale

1. GİRİŞ

Hewlett Packard Entreprise (2016) tarafından 2012 yılından itibaren yapılan çalışmada, son üç yılda haftalık başarılı siber saldırı sayısı ortalamasının 50'den 102'ye çıktığı, ortalama saldırılardan kurtarma süresinin 14 günden 24 güne çıktığı, yıllık ortalama kayıp maliyetinin ise 6,5 milyon dolardan 8,9 milyon dolara çıktığı belirtilmiştir. Bu tehditler ile mücadele etmek işletmelerin günlük sorumlulukları arasında yer almaktadır. Genellikle küçük kuruluşlar kaynak yetersizliği ya da farkındalık eksikliği nedenlerinden dolayı kendilerini güvence altına almaları çok zordur (Sorrentino, 2015). Bu etkenlerden içerisinde farkındalık her zaman daha etkin ve erken tedbir alınması konusunda ön plana çıkmaktadır (Wilson veHash, 2003: 9). Farkındalığın belirsizliği azaltması nedeniyle örgütlerin gerek ağ gerekse kullanımlar ilgili çalışanları bilgilendirmesi önemlidir (Bisson, 2015: 8) .

KOBİ'lerin yaşanan saldırılar sonucunda gelir kaybına, müşteri güven kaybına, yatırımcı güveninin azalmasının yanı sıra yapılan saldırıların büyüklüklerine göre de iflas etmeye kadar gidebilmektedir (Boateng ve Osei, 2013: 115). Bu düzeyde önemli bir konu üzerinde KOBİ'lerin karşılaşabilecekleri siber tehditlerle ilgili farkındalıkları araştırması bakımından bu çalışma önem taşımaktadır.

2.LİTERATÜR TARAMASI

Gizlilik, veri bütünlüğü, erişebilirlik (CIA) onlarca yıl bilgisayar güvenliğinin ve bilgi güvenliğinin modeli olarak kullanılmıştır (Whitman ve Mattord, 2012). CIA modelini ilk olarak 1975 yılında Saltzer ve Shroeder (1975) tarafından bilgiyi tehdit eden üç unsur olduğunu ortaya çıkarmıştır;

- ✓ Yetkisiz kişilerin bilgiye ulaşamaması (Gizlilik)
- ✓ Yetkisiz kişilerin bilgiyi değiştirememesi (Bütünlük)
- ✓ Bilgiye ulaşılabilirlik (Erişebilirlik)

CIA'ya alternatif olarak ilk kapsamlı model 1991 yılında Mccumber (1991) tarafından geliştirilmiştir. Bu model Mccumber'in Küpü olarak bilinmektedir. Bu model Milli Eğitim Standardı Bilgi Sistemleri Güvenliği Uzmanları (CNSS 4011) programının bir parçası olarak kullanılmaktadır (Committee on National Security Systems: National Information Assurance (IA) Glossary, 2010).

Maconach (2001) McCumber'in küpüne zaman boyutunu ve güvenlik önlemlerine kimlik doğrulama ve inkar edememeyi de ekleyerek geliştirmiştir.

Yulia ve Jeremy (2013) ''Reference Model of Information Assurance & Security'' adlı modelini oluşturmuştur. RMIAS dört bölümden oluşmaktadır.

- ✓ Bilgi sistem güvenliği yaşam döngüsü
- ✓ Bilgi taksonomisi boyutları
- ✓ Bilgi güvenlik boyutları
- ✓ Karşı güvenlik boyutu

Ölçeğin amacı KOBİ'lerin siber riskler karşısında bilgi güvenliği farkındalıklarını ölçmek olduğundan dolayı, bilgi güvenlik boyutları üzerinde duralmaktadır. Daha önce bahsedildiği üzere CIA güvenlik prensiplerinin temelini oluşturuyordu. Oysa günümüzde CIA gelişen yeni tehditleri kapsayamamaktadır (Cherdantseva, Hilton, Rana ve Ivins, 2013: 57). Güvenlik prensiplerinin boyutlarının geliştirilmesi için Bilgi Güvenliği Literatürü ve Sistem Mühendisliği literatürüyle ilgili yaptıkları araştırmalar sonucunda, günümüz tehditlerini de kapsayan Reference Model of Information Assurance & Security (RMIAS) modelini

geliştirmiştir. Yapılan analiz sonuçları literatürde güvenlik prensipleriyle ilgili ortak bir sonuca varılamadığı belirtilmekte ve bu da dört nedene bağlanılmaktadır (Cherdantseva, Hilton, Rana ve Ivins, 2013: 58).

- ✓ Aynı konuların farklı başlıklar altında sınıflandırılması
- ✓ Aynı isimle tanımlanmış güvenlik prensiplerinin farklı şekilde açıklanması
- ✓ Güvenlik prensiplerinin ayırt edici özelliklerinin olmaması
- ✓ Güvenlik prensipleriyle ilgili verilen maddelerin nitelik eksikleri (Bütünlük, sistem bütünlüğü ya da bilgi bütünlüğünü kapsayabilmektedir)

Yukarda bahsedilen nedenlerden dolayı güvenlik prensipleriyle ilgili literatürde ortak bir görüş olmadığından dolayı, Yulia ve Jeremy (2013) tarafından aşağıda belirtilen yol haritası sonucunda güvenlik prensiplerini yeniden tanımlandırılmıştır:

- ✓ Literatür taranarak güvenlik prensipleri kapsayıcı maddeler halinde listelendi.
- ✓ Bütün güvenlik prensipleri ayrıntılı ele alındı.
- ✓ İki anlamlı güvenlik prensipleri tek bir başlık altında toplanıp geliştirildi.

Science ve Direct (2016) dergisi tarafından yayınlanan makalede Bilgi güvenliğine ilişkin günümüze kadar gelen modellerin kapsamıyla ilgili inceleme yapılmıştır. Yapılan analiz sonucunda RMIAS modeli günümüze kadar yapılan en kapsayıcı model olduğu sonucuna varılmıştır (Cherdantseva, Rana, Ivins ve Hilton, 2016: 52). Bütün bu analizler sonucunda, RMIAS modelinde baz alınan güvenlik prensipleri maddelerine ilişkin anket soruları hazırlanmıştır.

RMIAS modelinde güvenlik prensipler 8 aşamadan oluşmaktadır;

Gizlilik: Bilgilerin yetkisiz kişilerden korunması olarak tanımlanmaktadır. Gizlilik ihlalini ise iletişim ya da bir dosyanın ifşa edilmesi sonucu oluştuğu belirtilmiştir (Knorr ve Rohrig 2015: 76).

Adalet Bakanlığınca hazırlanan Bilgi Güvenliği ve Kullanıcı Sorumluluğu ile ilgili raporda ise gizliliği kısaca bilginin yetkisiz kişilerin eline geçmemesi olarak tanımlanmaktadır(Adalet Bakanlığı, 2012: 12)

Tamlık-Bütünlük: Tamlık-Bütünlükten kastedilen, bilginin göndericiden çıktığı halde, tahribata uğramadan alıcıya ulaşmasıdır (Sınav, 2014: 59).

Erişebilirlik: Erişebilirlikten kastedilen, Bilişim sistemlerinin içeriden ya da dışarıdan, sistemi yavaşlatmaya yönelik saldırıların engellenmesidir (Yıldız, 2014: 60).

İzlenebilirlik ya da Kayıt Tutma: Alan Westin (1967) Gizlilik ve Özgürlük adlı kitabında, gizliliğin tanımını bireylerin kendileriyle ilgili kişisel bilgilerin başkalarına iletilmesiyle ilgili sahip oldukları haklar olarak tanımlamaktadır. Bu tanım izlenebilirliğin temelini oluşturmakta ve bütün bilgileri kapsayacak şekilde açıklanmaktadır.

İzlenebilirlik ya da kayıt tutma kısaca sistemin kullanıcıların yaptığı eylemlerden sorumlu tutulabilmesi için kaydını tutması olarak tanımlanmaktadır (Weitzner vd., 2008: 83).

Orijinallik-Güvenirlik: Ağ güvenliği için kimlik sorgulanması, göndericinin ve alıcının doğru kişi olup olmadığını sorgulamasıdır (Yıldız, 2014: 60).

Denetleme: Denetlemeden kastedilen "sistemin insan veya makineler tarafından yapılan tüm eylemlerin izlenebilirliğinin sağlanabilmesi" olarak tanımlanmaktadır(Cherdantseva, Hilton, Rana ve Ivins, 2013: 57).

İnkar Edememe: Bu veri sayesinde alıcı ve gönderici aldıkları mesajları gizleyememektedir. Özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde işlem görmektedir. Bunun yanı sıra belli bir potansiyel saldırıya karşı sistemi korumaya yönelik olduğu söylebilmektedir (Cherdantseva, Rana, Ivins ve Hilton, 2016: 50).

Mahremiyet: Ticari tüketici bağlamında mahremiyet, müşterilerin kişisel bilgilerinin korunması ve uygun şekilde kullanılması ve müşterilerin kullanımıyla ilgili beklentilerini karşılamasını gerektirmektedir (Perason, 2012: 220).

3.METODOLOJİ

3.1.Araştırmanın Amaçları

Bu araştırmanın üç amacı bulunmaktadır:

- ✓ KOBİ'lerin karşılaşabilecekleri siber tehditlerle ilgili bilgi farkındalıkları araştırmak.
- ✓ Bu farkındalığı ölçmek için ölçek geliştirmek.
- ✓ KOBİ'lerin bilgi güvenliği farkındalıklarıyla ilgili zayıf ve güçlü noktalarını görebilmelerini sağlamak için ölçek geliştirmek

3.2.Yöntem

Ölçeğin uygulanması için 2017 yılında Türkiye'nin Gaziantep ili sınırlarında faaliyet gösteren tüm kobi çalışanları evren olarak belirlenmiştir. Evren büyük olmasından dolayı örneklem alma yoluna gidilmiştir. Ölçek formu iki kısımdan oluşmaktadır. Birinci kısımda katılımcıların özelliklerini belirlemeye yönelik demografik sorularla birlikte kobilerin bilgi güvenliğine yönelik siber risklere karşı aldıkları yöntem ve uyguladıkları teknikleri belirleme yönelik sorulardan oluşmaktadır. Ölçeğin ikinci kısmında ise uzman görüşleri sonunda oluşturulan firmaların bilgi güvenliği ve farkındalığını belirlemeye yönelik 37 madde yer almaktadır. Hazırlanan bu form 800 kişiye uygulanmıştır. bazı ölçek formlarının rastgele ve eksik doldurulduğu fark edilmiştir. Bunun sonucunda rastgele ve eksik doldurulan ölçek formları araştırmaya dahil edilmemiştir. Analizler için kullanılacak ölçek form sayısı 756 olarak belirlenmiştir.

3.3. Verilerin Analizinde Kullanılan İstatistiksel Yöntemler

Araştırma için elde edilen verilerin analizi SPSS 21 istatistik paket programı kullanılarak yapılmıştır. Bağımlı ve Bağımsız gruplarda ikili karşılaştırma için t Testi, Korelâsyon Analizi, Madde Analizi, Faktör Analizi ve iç tutarlılığı belirlemek için Concbach Alfa katsayısı bu program paket programı kullanılarak hesaplanmıştır. Doğrulayıcı faktör analizi ve 5'li model uygunluğu indeks değerleri de AMOS 21 programı yardımıyla hesaplanmıştır. Beşli Likert Tipi ölçeği kullanılmıştır. Ölçeğin ikinci kısmında yer alan sorular "Kesinlikle katılmıyorum" ile "kesinlikle katılıyorum" arasında değişmekte ve ifadelerde bu derecelendirmeye göre değerlendirilmiştir.

3.4. Kobilerin Bilgi Güvenliği Farkındalığı Ölçeği'nin Geçerlilik Analizi

Bir ölçme aracının geçerliliğini sınamaya yönelik birçok ölçüt bulunmakla birlikte, bunlar genel olarak üç başlık altında toplanmaktadır (Karasar, 1995; Özgüven, 2000; Polit, Hungler, 1997; Tezbaşaran, 1996):

- ✓ İçerik/Kapsam geçerliği (content validity)
- ✓ Ölçüt-bağımı geçerliği (criterion-related validity)
- ✓ Yapı geçerliği (construct validity)

Bu çalışmada geliştirilen ölçek için kapsam, ölçüt ve yapı geçerliliği ayrı ayrı incelenmiştir.

3.4.1. Kapsam/İçerik Geçerliği

Kapsam geçerliğinin amacı, ölçme aracında bulunan maddelerin ölçülmek istenen alanı temsil edip etmediğini bir uzman gruba inceleterek anlamlı maddelerden oluşan bütün oluşturmaktır. Burada sözü edilen uzman kişi hem ölçeğin hazırlandığı bilm alanın iyi bilen hem de ölçek sorusu hazırlama teknik ve yöntemlerini bilen bir kişidir. Uzmanların öneri ve eleştirileri doğrultusunda ölçek yeniden yapılandırılmaktadır (Karasar, 1995; Özgüven 2000; Polit Hungler 1997; Tezbaşaran, 1996).

İçerik geçerliliği uzmanların yargılarına dayanan bir ölçüttür. Ölçeğin içeriğinin yeterli olduğunun garanti altına alacak objektif kriterleri yoktur. Uzmanların çoğunluğnun aynı fikirde olması bir gösterge olabilmektedir (Polit, Hungler 1997; Portney Watkin 1993). Bu kapsamda Kobi Çalışanlarının çalıştıkları firmanın bilgi güvenliği farkındalığını ölçmek için danışman Prof. Dr. Gülçimen Yurtsever ve bir araştırmacının görüşleri alınmış ve bu görüşler literatür araştırmasına da dayandırılarak ölçek geliştirilmiştir.

İkinci Bölümde açıklanan ve Cherdantseva, Rana, Ivins, ve Hilton (2016) tarafından geliştirilen "RMIAS" modeli araştırmanın modeli olarak kullanılmıştır İçeriğin boyutlarının belirlenmesi ölçek geliştirmedeki en zor kısımdır. Bu amaçla bir uzmanlar grubundan yararlanılmasına ve literatür desteğine ihtiyaç duyulmaktadır. Bu amaçla alanında uzman 3 bilişim sistem uzmanı, 2 öğretim görevlisi ve 1 araştırma görevlisiyle birlikte ölçek madeleri geliştirilmiştir. Yapılan görüşmeler sonucunda 41 olan taslak ölçek maddeleri 37 maddeye indirilmiştir. Katılımcıların ölçekte yer alan olumlu ifade içeren maddelere ait cevap puanları 1 ile 5 arasında değerler almış ve cevaplayıcıların ifadeleri 5'e yaklaştıkça önermeye katıldıklarını; 1'e yaklaştıkça ise maddeki ifadeye karşı olumsuz görüşe sahip olduklarını göstermektedir. Katılımcıların olumsuz ifade içeren maddere ait cevap puanları 5 ile 1 arasında tersten değerler almış ve katılımcıların ifadeleri 1'e yaklaştıkça önermeye katıldıklarını; 5'e yaklaştıkça ise önermeye katılmadıklarını göstermektedir.

Tablo 1. Ölçek Maddeleri

Kobilerin Bilgi Güvenliğiyle ilgili Farkındalıkları		
Gizlilik		
1	Knorr ve Rohrig (2015)	Firmamız, yetkimizin olmadığı dosyalara girişlerimizi engeller.
2	Australian Government Department of Defance Intelligence ve Security (2012)	Firmamızda, teknolojik cihazlarda (makina, bilgisayar ve benzeri) izinsiz erişimi engellemek adına gerekli önlemler bulunur.
3	Whitman ve Mattord (2014)	Firmamızda önemli bilgilerin gizliliğinin korunabilmesi için ''Bilgi sınıflandırması'' kullanılır.
4	Whitman ve Mattord (2014)	Firmamızda, önemli bilgilerin gizliliğinin korunabilmesi için ''Güvenli belge deposu'' na benzer önlemler bulunur.
5	Whitman ve Mattord (2014)	Firmamızda önemli bilgilerin gizliliğinin korunabilmesi için ''Genel güvenlik politikaları'' uygulanır.
6	Whitman ve Mattord (2014)	Firmamızda, önemli bilgilerin gizliliğini korunabilmesi için ''Bilgi saklama alanı'' kullanılır.
7	Whitman ve Mattord (2014)	Firmamızda, önemli bilgilerin gizliliğinin korunabilmesi için ''son kullanıcıların eğitimine'' önem verilir.
Tamlık		
8	Boateng ve OSEİ (2013)	Firmamız, internetten yüklenen bütün dosyaların virüs programıyla taranmasına önem verir.
9	Knorr ve Rohrig, 2015)	Firmamızda, müşterilerimle olan iletişimimde, herhangi bir verinin değiştirilmesi olasılığına karşı önlem alınır.
10	Australian Government Department of Defance Intelligence ve Security(2012)	Ciddi bir siber saldırı ile bilgilerimizin zarar görmesi durumunda firmamız önemli derecede etkileneceğini düşünürüm.
11	Jeucken (2005)	Firmamızda, verilerin izinsiz değiştirlmesi konusunda önlem alınır.

Erişebilirlik		
12	Chaptered Proffessional account's canada (2014)	Kullandığımız bilişim sistemlerinin herhangi bir unsurunun (yazılım veya donanım vb.) kendisinden beklenildiği şekilde çalışmaması işlerimizi önemli ölçüde yavaşlatır.
13	Boateng ve OSEI (2013)	Şirketimiz,mail aracılığıyla gelebilecek olan virüslerin sistemimize girmemesi için önlemler alır.
14	Knorr ve Rohrig (2015)	Şirketimiz, dosya erişimlerine ulaşma hızımız yavaşladığında önlem alır.
15	Boateng ve OSEI (2013)	Şirketimiz, mail aracılığıyla zararlı dosyaların sistememize girmemesi için önlemleri göz ardı eder.
İzlenebilirlik Yada Kayıt tutma		
16	Yildirim, Akalp, Aytaç, Bayram (2011)	Firmamızda bilgi sistemlerine üçüncü taraf (dışarıdan) erişim, üst düzey bir yöneticinin onayını gerektirir.
17	Boateng ve OSEI (2013)	Firmamızda evrakların imha işlemi verinin izlenebilirliğini azaltmak için kullanılır.
18	Boateng ve OSEI (2013)	Firmamız verilerin kopyalamasını engeller.
19	Yan, Qian, Sharif ve Tipper, (2012)	Firmamız, dosya yada önemli bir evrak değiştirildiği zaman, değişiklik yapan kullanıcıyı görebilir.
Orijinallik-Güvenirlik		
20	Keller, Powell, Horstmann, Predmore ve Crawford (2005)	Firmamız, siber güvenlik açısından belirlenmiş riskler olduğunu düşünür ve bunlara karşı önlem alır.
21	Chaptered Proffessional account's canada (2014)	Firmamız, önemli evrakların değiştirilme ihtimaline karşı önlem alınır.
22	Kese ve Güldüren (2015)	Firmamız, bilgisayarımıza casus yazılım yüklenmesini engellemek için önlem alır.
23	Meb (2013)	Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.
Denetleme		
24	Yan, Qian, Sharif ve Tipper, (2012)	Firmamız, sistemdeki arızanın kaynağını tarihsel kayıtlardan çıkartabilir.
25	Yan, Qian, Sharif ve Tipper, (2012)	Firmamız sistemde ki değişikliklerden dolayı doğabilecek sorunları engellemek için önlem alır.
26	Yildirim, Akalp, Aytac ve Bayram (2011)	Firmamızda, güvenlik politikalarımızı ihlal eden çalışanlar için resmi bir disiplin süreci vardır.
27	Boateng ve OSEI (2013)	Firmadaki bilgisayarıma Mp3, video benzeri dosyaları indirebilirim.
İnkar Edememe		
28	Cherdantseva, Rana, Ivins ve Hilton (2016)	Firmamız, önemli bilgiler paylaştığımızda karşıdan yazılı onay almamızı ister.
29	Zhou ve Gollmann (1997)	Yazılı onayların, ileride doğabilecek hukuksal problemleri engelleyeceğinin farkındayım.
30	Lagou ve Chondrokoukis (2009)	Firmamızda, Dijital imzaya önem gösterilir.
31	(Zhou ve Gollmann, 1997)	Firmamız, önemli bir evrak silindiği zaman, işlemi yapan kullanıcıyı kayıtlardan bulamaz.
Mahremiyet		
32	Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) ve Avrupa Konseyi (1980)	Firmamız, müşterilerimizin rızası olmadan bilgilerini başka amaçlarla kullanmaz.
33	Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) ve Avrupa Konseyi (1980)	Firmamız, müşterilerimin bilgilerini başka kurumlarla paylaşmadan önce ilgili kişiye bilgi verir.
34	Chaptered Proffessional account's canada (2014)	Firmamız, müşterilerimizin kişisel bilgilerini olası tehditlere karşı korur.
35	Keser, Güldüren (2015)	Kişisel mahremiyetin ne olduğunu biliyorum.
36	Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) ve Avrupa Konseyi (1980)	Müşterimle olan ilişkilerimde kişisel mahremiyete göre hareket ederim.
37	Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) ve Avrupa Konseyi (1980)	Firmamız, müşterilerimin bilgilerini başka kurumlarla paylaşmadan önce ilgili kişiye bilgi verir.

3.4.2. Ölçüt Geçerliği

Hemzaman/eşzaman geçerliliği yöntemi kullanılmıştır. Bu çalışmada 50 kişilik örneklem grubu üzerinde, 2014 yılında Akademisyenler üzerinde Bilgi güvenliği farkındalığı ölçeği

(ABGFÖ) ile Bilgi güvenliği farkındalığı ölçeği aynı anda uygulanmış ve elde edilen sonuçlar arasında korelasyon hesaplanmıştır. Koreleason değeri r = 0,407 olup istatistiksel olarak anlamlıdır (p=0,003<0,05). Elde edilen bu korelasyon değerine göre geliştirilen ölçek ile daha önceki ölçek arasında pozitif yönde ve orta düzeyde bir ilişki olduğu söylenebilir. Bu iki ölçek arasındaki korelasyon değerleri Tablo 2'de verilmiştir.

Tablo 2. Ölçüt geçerliliği korelasyon analizi sonuçları

		KBGFÖ	ABGFÖ
KBGFÖ	Pearson Korelasyon	1	
	N	50	
ABGFÖ	Pearson Korelasyon	,407**	1
	P	,003	
	N	50	50

**. Korelasyon değeri %1 önem seviyesinde anlamlıdır.

3.4.3.Yapı Geçerliliği

Yapı geçerliliği, ölçeğin ilgili kavram ya da kavramsal yapının tümünü ölçme yeteneğini göstermektedir (Portney, Watkins, 1993). Bir ölçeğin ve ondan elde edilen puanın gerçekte ne anlama geldiğini araştırma sürecidir. Bu süreç, ölçeğin ölçtüğü faktörler incelenerek ya da geçerliği araştırılan ölçeğin diğer ölçek ve ölçülerle olan ilişkisini araştırarak gerçekleştirilir. Her defasında ölçekle ilgili yeni bir parça bilgi elde edilerek, yığılmalı bir şekilde ölçeğin yapısı ve puanın anlamı hakkında bilgiler elde edilmektedir (Özgüven,2000). Bir ölçeğin yapı geçerliğini değerlendirmek üzere faktör analizi uygulanmaktadır (Karasar, 1995: Pcircc, 1995;Polit, Hungler, 1997; Portney, Watkins, 1993).

3.4.3.1. Açımlayıcı Faktör Analizi (AFA)

Açımlayıcı Faktör Analizi uygulamayabilmek için iki ön koşul bulunmaktadır: Örneklem büyüklüğünün yeterli olması ve verinin çok değişkenli Normal dağılımlı olmasıdır. Bu koşulları sınamak amacıyla örneklem büyüklüğünün yeterliği için Kaiser Meyer Olkin (KMO) katsayı değeri hesaplanırken, normallik şartı için Barlett Küresellik testinin manidar olup olmadığı araştırılmaktadır. Her veri grubuna KFA faktör analizi uygulanmaz. Bir veri grubuna faktör analizi uygulanabilmesi için verinin faktör analizine uygunluğu ve örneklemin yeterli olması gerekmektedir. Bu amaçla KFA uygulanırken Bartlett (1950) tarafından geliştirilen "Bartlett Küresellik Testi" ve Kaiser (1970) tarafından bulunan Kaiser-Meyer-Olkin (KMO) testi sonuçlarına bakılır (Aydın ve Yayla, 2018: 77). Örneklem büyüklüğünün yeterliliği için KMO değerinin en az 0.60 olması gerekmektedir (Büyüköztürk, 2003: 120). KMO değeri bu sayıdan küçük ise analize devam edilmemelidir. Ancak KMO değeri 0,90 ve üzeri ise örneklem büyüklüğünün faktör analizi için mükemmel olduğu yorumlanmaktadır (Tavşancıl, 2005; Çokluk ve ark., 2010).

Ölçeğin deneme çalışmasında Tablo 3'de görüleceği üzere KMO değeri 0,942 olarak tespit edilmiştir. Barlett küresellik testi sonucu manidar olarak bulunmuştur ($\chi^2 = 12536,497$ sd=666; p=0,00<0,01). Bu sonuçlar, pilot çalışması için elde edilen örneklem verisinin büyüklüğünün faktör analizi için mükemmel ve örneklem verisinin dağılımın çok değişkenli normal dağılımlı olduğu sonucuna ulaşılmıştır.

Tablo 3. KMO ve Bartlett Testi Sonucları

Kaiser-Meyer-Olkin Örneklem Yeterliliği Ölçüsü		,942
Bartlett Küresellik Testi	Ki-Kare Değeri	12536,497
	sd	666
	p	,000

Ölçek geliştirme aşaması öncesinde araştırmacılar tarafından belirlenen tek faktörlü (genel görüş) yapıya uygun olarak geliştirilmek istenmiş ve bu sebeple öncelikle madde analizi birinci örneklem grubuna uygulanmıştır. Madde-toplam puan korelasyonu, ölçek maddelerinden alınan puan ile bütün test puanı arasındaki ilişkinin incelenmesine dayanan tutarlılık hesaplama yöntemidir (Tezbaşaran, 1996). Madde toplam test korelasyonu, test maddelerinden alınan puanlar ile testin toplam puanı arasındaki ilişkiyi açıklamaktadır (Büyüköztürk, 2004). Bu değerin yüksek olması, ölçme aracının iç tutarlılığının yüksek olduğu anlamına gelmektedir. Ölçeğe ilişkin madde analizi sürecinde madde-toplam korelasyonu 0,30 ve altındaki maddelerin ölçekten atılması uygun görülmektedir (Geuens and Pelsmacker, 2002). Bunun yanında, Büyüköztürk (2002) madde analizi ile madde belirlenmesinde madde-toplam korelasyon katsayısı $r \geq 0,40$ değerinin çok iyi maddelere ve $0,30 \geq r \geq 0,39$ iyi maddelere ait olacağını ifade etmektedir. Bu ölçek için yapılan madde analizi sürecinde, bu düzey "0,40" olarak belirlendiğinden, bu koşulu sağlamayan 4 maddenin (S2, S14, S17 VE S18), ölçeğin ölçmesi istenen durumu ölçmeye olan katkısının az olduğu düşünüldüğünden ölçekten çıkarılmasına karar verilmiştir. Kalan 33 maddenin madde-toplam korelasyonları $0,50 \leq r \leq 0,81$ arasında değişmektedir. Daha sonra ölçeğin ön uygulama verilerinden elde edilen toplam puanlar hesaplanmıştır. Ölçek maddelerinin % 27 alt-üst gruplar arası (N1-n1 =102, N1-n2 =102) ayırt ediciliğine, bağımsız gruplar için t testi yardımıyla bakılmıştır. Yapılan analiz sonucunda 37 maddenin her birinin t testi sonuçlarına göre istenilen düzeyde ($p<0,01$) ayırt edici olduğu görülmüştür. Madde analizi sonucunda ölçekte yer alan 37 maddenin analiz sonuçları Tablo 4'de sunulmaktadır.

Tablo 4. Madde Analizi

Madde	Grup	N	Ortalama	Standart Sapma	t- değeri	p	Madde Toplam Korelasyonu
S1	Alt	102	2,4216	1,26206	-12,167	0,000	,595
	üst	102	4,2059	,77509			
S2	Alt	102	2,1863	,93056	-19,152	0,000	,232
	üst	102	4,3627	,67177			
S3	Alt	102	2,5294	,95135	-15,223	0,000	,648
	üst	102	4,1961	,56357			
S4	Alt	102	2,1667	1,04439	-20,233	0,000	,756
	üst	102	4,5686	,58884			
S5	Alt	102	2,5784	1,06647	-10,991	0,000	,583
	üst	102	4,0686	,85896			
S6	Alt	102	2,1078	,75658	-23,179	0,000	,812
	üst	102	4,3235	,59970			
S7	Alt	102	2,3725	1,06168	-16,232	0,000	,718
	üst	102	4,3824	,66069			
S8	Alt	102	2,7549	1,14698	-10,923	0,000	,504
	üst	102	4,2353	,74696			
S9	Alt	102	2,6765	,93514	-14,084	0,000	,634
	üst	102	4,2745	,66238			
S10	Alt	102	2,5392	1,06865	-13,736	0,000	,621
	üst	102	4,2549	,67025			
	üst	102	4,1863	,90903			

Madde	Grup	N	Ortalama	Standart Sapma	t- değeri	p	Madde Toplam Korelasyonu
S11	Alt	102	2,5294	1,01187	-13,842	0,000	,628
	üst	102	4,3039	,65686			
S12	Alt	102	2,7157	,82507	-14,856	0,000	,622
	üst	102	3,9608	,85506			
S13	Alt	102	2,8529	,89439	-10,583	0,000	,717
	üst	102	3,8922	,96377			
S14	Alt	102	2,1078	,75658	-7,982	0,000	,248
	üst	102	4,2157	,63911			
S15	Alt	102	2,8529	1,00884	-21,495	0,000	,630
	üst	102	3,8333	,89091			
S16	Alt	102	2,8431	,79285	-7,357	0,000	,796
	üst	102	4,0098	,94915			
S17	Alt	102	2,1176	1,01761	-9,527	0,000	,292
	üst	102	4,1569	1,06933			
S18	Alt	102	2,3431	1,04829	-13,952	0,000	,257

3.4.3.2. Doğrulayıcı Faktör Analizi (DFA)

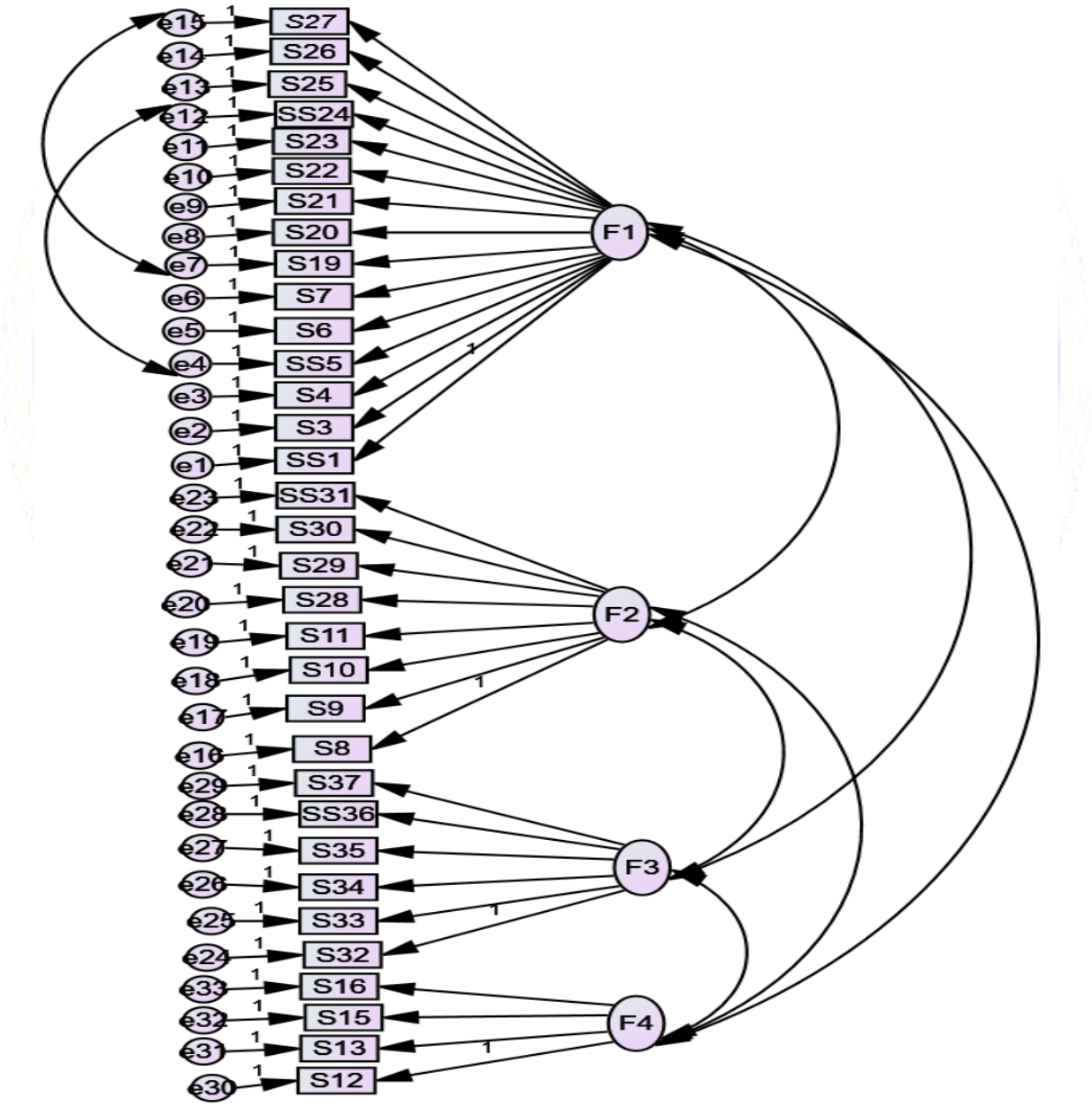
DFA Önceden oluşturulan bir model aracılığıyla gözlenen değişkenlerden yola çıkarak gizli değişken (faktör) oluşturmaya yönelik bir işlemdir. Genellikle ölçek geliştirme ve geçerlilik analizlerinde kullanılmakta veya önceden belirlenmiş bir yapının doğrulanmasını amaçlamaktadır. Çok sayıda gözlenen veya ölçülen değişken tarafından temsil edilen ve gizli yapıları içeren çok değişkenli istatistiksel analizleri tanımlamak amacıyla kullanılmaktadır. Doğrulayıcı faktör analizi, açıklayıcı faktör analizi ile belirlenen faktörlerin, hipotez ile belirlenen faktör yapılarına uygunluğunu test etmek üzere yararlanılan faktör analizidir. Açıklayıcı faktör analizi, hangi değişken gruplarının hangi faktör ile yüksek düzeyde ilişkili olduğunu test etmek için kullanılırken, belirlenen sayıda faktöre katkıda bulunan değişken gruplarının bu faktörler ile yeterince temsil edilip edilmediğinin belirlenmesi için doğrulayıcı faktör analizinden faydalanılmaktadır (Aytaç ve Öngen, 2010: 16). Özetle, yapısal eşitlik modellerinde teoride var olan kavramsal model, veri yardımı ile test edilmeye çalışılmaktadır. Doğrulayıcı faktör analizi, genellikle ölçek geliştirme ve geçerlik analizinde kullanılmakta ve önceden belirlenmiş bir yapının doğruluğunu belirlemeyi amaçlamaktadır. Bu amaçla açımlayıcı faktör analizi sonunda elde edilen 4 faktörlü yapının geçerliliğini sınamak için ikinci örneklem grubuna (N2=378) DFA uygulanmıştır. Literatürde açımlayıcı ve doğrulayıcı faktör analizinin farklı örneklem gruplarına uygulanması önerilmektedir. (Kabakçı vd., 2012; Wang vd., 2014; Çakıroğlu, Gökoğlu ve Çebi, 2015).

Açımlayıcı faktör analizi ile önceden belirlenen modellerin veriyi ne kadar iyi açıkladığı doğrulayıcı faktör analizinde uyum istatistikleri ile belirlenir. Modellerin uyumunu test eden birden fazla uyum istatistiği (fit statistic) vardır. Bu uyum istatistikleri, ileri sürülen modellerin parametreleri ile örnek verilerden elde edilen istatistiklerin uygunluğunu test etmektedir. Eğer model verilere uymuyorsa reddedilmektedir. İleri sürülen model reddedilemiyorsa, model gözlenen verilerin altında yatan nedensel yapıyı açıklama yeteneğine sahiptir (Özdamar, 2010: 251-252). Ki kare testi ile modelin genel uyumuna bakılır. Model uyumunun belirlenmesinde, başlangıç uyum indeksi olarak ki-kare uyum iyiliği indeksine (chi-square goodness of fit) bakılmaktadır. Ki-kare testi, veriyle model arasındaki uyumun testidir. Ki karenin anlamlı olmaması ve CMIN/DF = χ 2 /sd $\leq$ 5 olması modelin uyumluluğunu göstermektedir. Ki kare uyum iyiliği indeksi ile birlikte, Artırmalı Uyum İndeksi (Incremental Fit lndex, IFI), Karşılaştırmalı Uyum İndeksi (Comparative Fit Index,

CFI), Yaklaşık Hataların Ortalama Karekökü (Root Mean Square Error of Approximation, RMSEA), İyilik Uyum İndeksi (Goodness Of Fit Index, GFI), Ortalama Hataların (Kalıntıların) Karekökü (Root Mean Square Residual, RMR) de sık kullanılmaktadır. Aşağıdaki tabloda, uyum değerleri ve uyum aralıkları özetlenmiştir (Schermelleh Engel ve diğ., 2003).

Tablo 5. Uyum Değerleri ve Uyum Aralıkları

Model Uyum Kriteri	**İyi Uyum**	**Kabul Edilebilir Uyum**
x2 Uyum Testi	0,05<p=<1	0,01<p=<0,05
CMIN/SD	x2/sd≤3	x2/sd≤5
IFI	0,95≤IFI	0,90≤IFI
CFI	0,97≤CFI	0,95≤CFI
RMSEA	RMSEA≤0,05	RMSEA≤0,08
GFI	0,90≤GFI	0,85≤GFI
RMR	0<RMR≤0,05	0<RMR≤0,08



Şekil 1. DFA Modeli

Doğrulayıcı faktör analizi modeli Şekil 1 ile verilmiştir. Bu modele ait uyum indeks değerleri Tablo 6 ile verilmiştir. Tablo 6 incelendiğinde bu modele ait χ^2/df değerinin 1,937 olduğu görülmektedir $\chi^2 = 943{,}216\ ve\ df = 487$) bu değer 3'den küçük olduğu için modelin uyumu iyi olarak yorumlanabilir. Benzer şekilde IFI ve RMSEA değerleri sırasıyla 0,951 (≥0,95) ve 0,050 (≥0,050) olarak hesaplanmıştır. Hesaplanan her iki uyum indeks değeri için modelin uyumu iyi olarak kabul edilmektedir. Diğer uyum değerleri olan GFI, CFI ve RMR değerleride sırasıyla 0,863(≥0,85), 0,950 (≥0,95) ve 0,055 (0<RMR<0,08) olarak tespit edilmiştir. Bu üç uyum değerine gore, elde edilen modelin kabul edilebilir uyum değerlerine sahip olduğunu ortaya koymaktadır.

Tablo 6. DFA Modeline Ait Uyum İyiliği Değeri

Uyum Kriterleri	χ^2/df	GFI	IFI	CFI	RMSEA	RMR
Değerleri	1,937	0,863	0,951	0,950	0,050	0,055
Uyum İyiliği Durumu	İyi	Kabul edilebilir	iyi	Kabul Edilebilir	İyi	Kabul Edilebilir

Tablo 7. Faktörler Arası Korelasyon Değerleri

	F1	F2	F3	F4
F1	1			
F2	0,588*	1		
F3	0,562*	0,618*	1	
F4	0,235*	0,301*	0,292*	1

Tüm faktörler arası elde edilen modele göre hesaplanan korelasyon değerleri Tablo 7 ile verilmiştir. Bu değerler incelendiğinde faktörler arası hesaplanan korelasyon değerlerinin (p<0,05) istatistiksel olarak anlamlı olduğu ve faktörler arası korelasyonların 0,235 ile 0,618 arasında değiştiği görülmektedir. En yüksek korelasyon değeri F2 ve F3 faktörleri arasında olup r=0,618'dir. En düşük korelasyon ise F1 ile F4 arasında olup r=0,235'dir.

3.5. Kobilerin Bilgi Güvenliği Ölçeği'nin Güvenirlilik Çalışması

KBGFÖ'nin güvenirliği iç tutarlılık Cronbach Alpha yöntemi ile hesaplanmıştır. Likert tipi ölçek geliştirme sürecinin temel varsayımlarından biri, ölçülmek istenen tutumla ölçekte yer alan her bir maddenin monotonik bir ilişkiye sahip olmasıdır. Başka bir ifadeyle herbir maddenin, ölçeğin ölçmek istediği tutumla aynı yönde olması gerekmektedir (Tavşancıl, 2002: 152). Bunun için iç tutarlılık analizi kapsamında Likert tipi ölçeklerde güvenirlik düzeyini belirlemek için Cronbach tarafından geliştirilen Alpha katsayısı kullanılması uygundur. Cronbach Alpha katsayısı (1,00-0,80: Yüksek; 0,79-0,60: İyi; 0,59-0,40: Düşük; 0,39-0,00: Güvenilir değil) ne derece yüksek ise ölçekte yer alan maddeler birbirleriyle o derece tutarlıdır ve ölçekte yer alan her bir madde ölçeğin geneliyle aynı amaca hizmet etmektedir şeklinde yorumlanmaktadır (Tezbaşaran, 1996).

Kobilerin bilgi güvenirliği farkındalığını ölçmek amacıyla bu çalışmada hazırlanan ölçeğin genel güvenirliği ile bu ölçek içerisinde yer alan dört faktöre ait Croncbach Alpha güvenirlilik değerleri Tablo 8 ile verilmiştir. KBGFÖ ölçeğinin genel güvenirliği 0,954, Birinci faktörün 0,947, ikinci faktörün 0,927, üçüncü faktörün 0,923 ve dördüncü faktörün 0,924 olduğu tespit edilmiştir. Bu değerler dikkate alındığında ölçeğin oldukça güvenilir olduğu sonucuna varılmıştır. Ölçek içerisinde yer alan tüm maddelerin madde toplam korelasyon değerleri 0,50'nin üzerindedir. Madde-toplam korelasyonunun yorumlanmasında .30 ve daha yüksek olan maddelerin, bireyleri ölçülen özellik bakımından iyi derecede ayırt ettiği (Büyüköztürk, 2004) göz önüne alındığında, madde-toplam korelasyonlarının yeterli düzeyde olduğu görülmektedir.

Tablo 8. BGFA Ölçeğinde Yer Alan Maddelerinin ve Alt Boyutlarının Güvenirlilik Değerleri

Faktör	Madde No	Madde Toplam Korelasyonu		Cronbach's Alpha Güvenirlilik Katsayısı (α)			
		Faktör	Ölçeğin (Genel)	Faktörden Madde Silinirse	Ölçekten Madde Silinirse	Faktörlerin	Ölçeğin
F1	S3	,728	,624	,943	,953	,947	,954
	S20	,778	,719	,942	,952		
	S6	,787	,783	,942	,953		
	S7	,742	,689	,943	,953		
	S5	,668	,560	,944	,953		
	S24	,699	,604	,944	,953		
	S23	,752	,718	,942	,953		
	S4	,760	,712	,942	,953		
	S25	,715	,655	,943	,953		
	SS1	,666	,557	,944	,953		
	S19	,657	,558	,945	,953		
	S21	,719	,699	,943	,953		
	S27	,708	,703	,943	,953		
	S26	,694	,687	,944	,953		
	S22	,682	,699	,944	,953		
F2	S29	,774	,501	,916	,953	0,927	
	S10	,793	,643	,915	,953		
	S8	,718	,528	,921	,953		
	S9	,750	,659	,918	,953		
	S31	,701	,547	,922	,953		
	S11	,759	,639	,917	,953		
	S30	,733	,594	,919	,953		
	S28	,792	,702	,915	,953		
F3	S34	,729	,593	,916	,953	,923	
	S32	,761	,637	,912	,953		
	S33	,797	,666	,907	,953		
	S36	,767	,609	,911	,953		
	S37	,807	,636	,905	,953		
	S35	,813	,706	,905	,953		
F4	S16	,835	,525	,898	,954	,924	
	S13	,829	,684	,900	,954		
	S12	,825	,556	,902	,953		
	S15	,809	,749	,907	,953		

Madde	Grup	N	Ortalama	Standart Sapma	t- değeri	p	Madde Toplam Korelasyonu
S19	Alt	102	2,1765	,96894	-13,416	0,000	,588
	üst	102	3,8137	,78008			
S20	Alt	102	2,3922	,86924	-13,293	0,000	,746
	üst	102	4,3627	,71462			
S21	Alt	102	2,3725	1,07096	-17,686	0,000	,710
	üst	102	4,3529	,66967			
S22	Alt	102	2,5098	,94130	-15,835	0,000	,700
	üst	102	4,5784	,62038			
S23	Alt	102	2,0098	,93866	-18,532	0,000	,729
	üst	102	4,3529	,69861			
S24	Alt	102	2,6275	1,16824	-20,224	0,000	,626
	üst	102	4,4020	,60132			
S25	Alt	102	2,2549	,87525	-13,640	0,000	,666
	üst	102	4,3627	,89873			
S26	Alt	102	2,5196	1,03149	-16,969	0,000	,688
	üst	102	4,4510	,60734			
S27	Alt	102	1,9902	,88435	-16,296	0,000	,720
	üst	102	4,3333	,80016			
S28	Alt	102	2,5686	,91748	-19,842	0,000	,677
	üst	102	4,3333	,74904			
S29	Alt	102	2,7843	1,21564	-15,048	0,000	,473
	üst	102	4,1471	,69506			
	Üst	102	4,7059	,45790			
S30	üst	102	2,8431	1,08769	-9,829	0,000	,574
	Üst	102	4,3431	,66742			
S31	üst	102	2,6569	1,08541	-11,871	0,000	,525
	Üst	102	4,2157	,75291			
S32	üst	102	2,9118	1,08183	-12,384	0,000	,623
	Üst	102	4,5196	,74102			

Madde	Grup	N	Ortalama	Standart Sapma	t- değeri	p	Madde Toplam Korelasyonu
S33	Alt	102	2,6569	1,05769	-15,213	0,000	,657
	üst	102	4,5196	,64070			
S34	Alt	102	2,7353	1,09839	-11,891	0,000	,584
	üst	102	4,2941	,73912			
S35	Alt	102	2,6765	1,03562	-15,851	0,000	,692
	üst	102	4,5098	,54035			
S36	Alt	102	2,7745	1,06154	-12,443	0,000	,597
	üst	102	4,3922	,77276			
S37	Alt	102	3,0392	1,04286	-14,779	0,000	,614

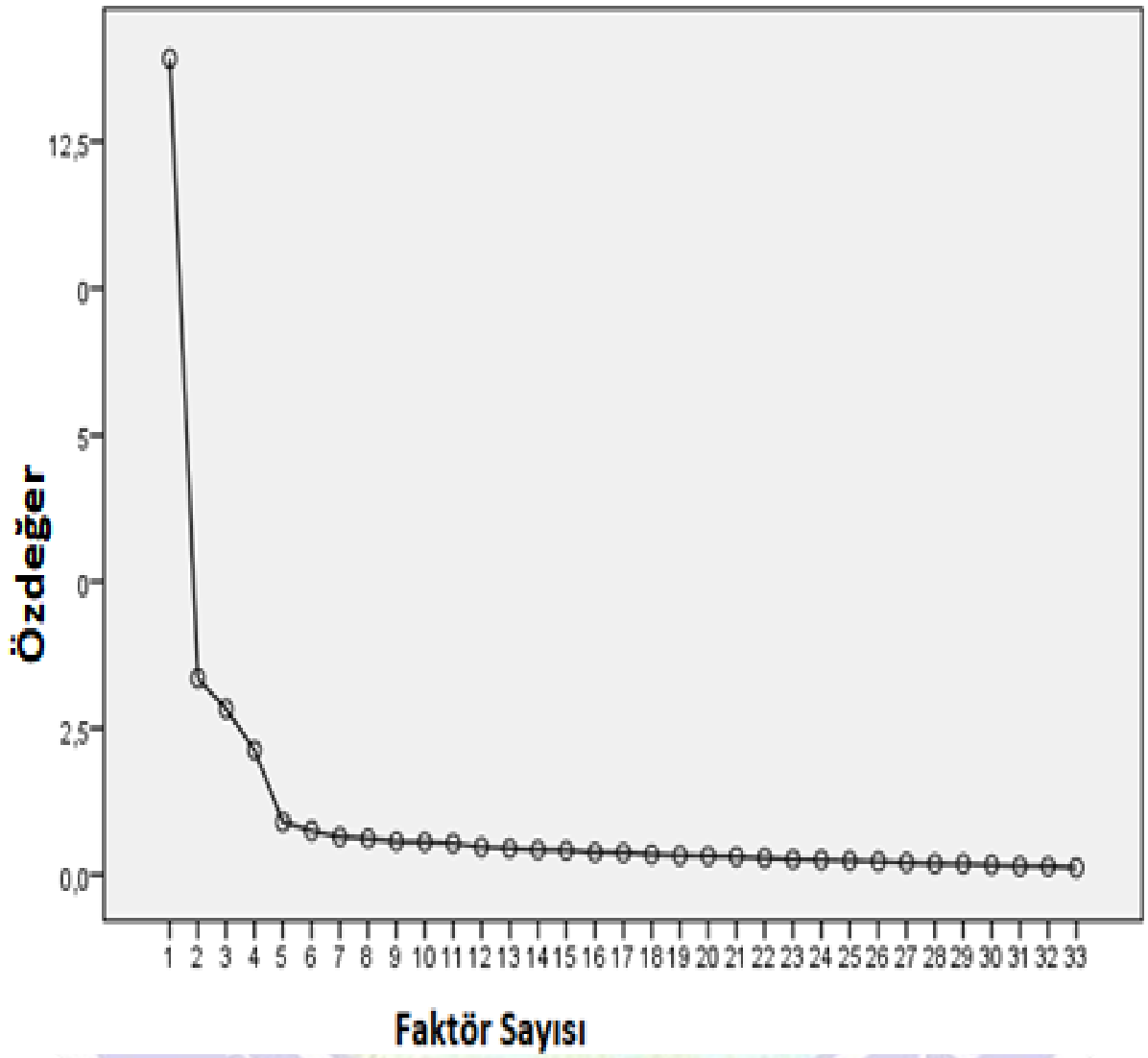
Maddeler arasındaki ilişkileri az sayıda ve en etkin şekilde ortaya koyabilecek faktör sayısını belirlemek için iki kriterden yararlanılmıştır. Bunlar, faktör özdeğerlerine dayalı olarak faktör özdeğer büyüklüğü ve birikimli çizgi grafiği kriterleridir. Bryman ve Cramer (1999), özdeğeri 1 veya 1'den büyük olan faktörlerin önemli faktör olarak nitelendirilmesi gerektiğini belirtmiştir. Bununla birlikte Büyüköztürk (2007) çizgi grafiğin maddelerin özdeğerlerinin birleştirilmesi sonucunda elde edildiğini, bu nedenle grafikte görülebilecek hızlı düşüşlerin (kırılma noktalarının) faktör sayısını vereceğini belirtmektedir.

Tablo 9. Faktör Toplam Varyansı

Bileşen	Başlangıç Özdeğerleri			Kareler Toplam Rotasyonu		
	Toplam	Açıklanan Varyans Yüzdesi	Birikimli Varyans Yüzdesi %	Toplam	Açıklanan Varyans Yüzdesi	Birikimli Varyans Yüzdesi %
1	13,917	42,172	42,172	8,458	25,630	25,630
2	3,353	10,159	52,332	5,789	17,542	43,172
3	2,825	8,562	60,894	4,565	13,834	57,006
4	2,127	6,444	67,337	3,409	10,331	67,337
5	,900	2,726	70,063			
32	,140	,423	99,640			
33	,119	,360	100,000			

Açımlayıcı faktör analizinde temel bileşenler yöntemi ve dik döndürme sonunda faktör özdeğerleri ve faktörlerin toplam varyansı açıklama oranları Tablo 8 ile verilmiştir. Tablo 9 incelendiğinde özdeğeri birden büyük dört faktörlü yapının olduğu tespit edilmiştir. Bu yapı toplam varyansın %67,33'nü açıklamaktadır. Sosyal bilimlerde yürütülen çalışmalarda toplam varyans oranının % 40 ile % 60 arasında değer alması ölçeğin faktör yapısının güçlülüğüne işaret etmektedir (Tavşancıl, 2002). Bu durum ölçeğin toplam varyans oranının yeterli bir değere sahip olduğunu göstermektedir. Bu çalışmada elde edilen %67,33'lük toplam varyans oranının %42'si Faktör 1, %10'16'sı Faktör 2, %8,56'sı Faktör 3 ve %6,44'ü Faktör 4 tarafından açıklanmaktadır. Faktör sayısını belirleme için ayrıca çizgi grafiği incelemesi de yapılmıştır. Araştırmada geliştirilen ölçeğe ait çizgi grafiği şekil 10 ile verilmiştir. Şekil 2 incelendiğinde çizgi grafiğinde yüksek ivmeli hızlı düşüşlerin yaşandığı bileşenlerin 1, 2, 3 ve 4 numaralı faktörler olduğu, 5 numaralı faktörden itibaren grafiğin yatay bir görünüm aldığı

anlaşılmaktadır. Buna göre ölçeğin içerdiği anlamlı faktör sayısının dört olduğu görülmektedir.



Şekil 2. Çizgi Grafiği

Faktör analizinde maddelerin en yüksek faktör yükü 0,45'den küçük ve birden fazla faktörde yer alıp birbirinden ayırt edilemeyecek kadar yakın (en yüksek iki faktördeki madde yükü arasındaki fark 0,10'dan küçük) olan maddeler varsa ölçekten çıkarılması önerilmiştir (Büyüköztürk, 2002: 474-479). Bununla birlikte bu aşamada aynı zamanda maddelerin ortak faktör varyans değerleri de incelenmelidir. Ortak varyans, ölçek içerisindeki bir maddenin diğer maddelerle paylaştığı varyans miktarıdır (Hair ve ark, 1998: 365). Ölçekte yer alan her bir madde için hesaplanan bu değerin 0,50'inin altında olması durumunda o maddenin ölçekten çıkarılması önerilmektedir (Kalaycı, 2010: 342; Çokluk ve diğ., 2010: 194). Geliştirilen ölçekteki maddelerin faktör yükleri ve ortak faktör varyans değerleri Tablo 10 ile verilmiştir.

Tablo 10. Faktör Yükleri ve Ortak Faktör Varyansı

	Rotasyonlu Bileşen Matrisi					
	Madde	Faktör Yükleri				Ortak Faktör Varyansı
		1	2	3	4	
FAKTÖR 1	S3	,764	,075	,130	,109	,507
	S20	,763	,173	,206	,140	,618
	S6	,763	,328	,197	,095	,643
	S7	,761	,152	,169	,148	,589
	S5	,758	,066	,016	,100	,737
	S24	,756	,087	,081	,113	,653
	S23	,735	,266	,227	,001	,627
	S4	,734	,217	,207	,117	,700
	S25	,699	,238	,110	,114	,733
	SS1	,696	,100	,110	,028	,679
	S19	,675	,064	,229	-,051	,821
	S21	,664	,221	,314	,061	,793
	S27	,658	,199	,264	,211	,767
	S26	,635	,261	,308	,022	,851
	S22	,577	,371	,267	,074	,515
FAKTOR 2	S10	,084	,861	,080	,015	,674
	S29	,209	,794	,215	,111	,592
	S8	,120	,761	,161	,084	,547
	S9	,277	,759	,159	,149	,663
	S31	,215	,748	,139	-,042	,599
	S11	,227	,742	,179	,211	,571
	S30	,206	,739	,220	,035	,567
	S28	,259	,736	,303	,156	,586
FAKTÖR 3	S34	,225	,143	,808	,143	,725
	S32	,251	,221	,807	,088	,755
	S33	,330	,164	,785	,137	,639
	S36	,186	,246	,781	,149	,626
	S37	,241	,282	,722	,136	,772
	S35	,342	,340	,721	,025	,770
FAKTOR 4	S12	,127	,140	,128	,894	,744
	S13	,150	,048	,119	,868	,753
	S16	,205	,137	,091	,867	,727
	S15	,052	,101	,145	,856	,677

Tablo 10 incelendiğinde, Temel Bilşenler Yöntemi ve Dik döndürme (orthogonal) sonrası ölçek maddelerinin 4 faktörde, 0,577 ile 0,894 faktör yükleri aralığında toplandığı görülmektedir. Ölçekte yer alan 33 maddenin en yüksek faktör yük değerleri 0,45'in altında olan madde tespit edilememiştir. Bu maddelerin faktör yükleri bakımından en yüksek iki faktördeki faktör yükleri arasındaki fark 0,1'den büyüktür. Ayrıca maddelerin ortak varyans değeri 0,507 ile 0,851 arasında olduğu hesaplanmıştır. Bu aşamada ölçekten herhangi bir maddenin çıkarılması gerekmemektedir. Analiz sonucunda Faktör 1'in 15 maddeden, Faktör 2'nin 8 maddeden, Faktör 3'ün 6 maddeden, ve Faktör 4'ün 4 maddeden, oluştuğu tespit edilmiştir.

Faktörlerin içindeki maddelere bakıldığında en fazla maddeye sahip olan faktör, faktör adları olarak kullanılmıştır. Faktör I'de en fazla faktör yük değerine sahip olan madde 3'ün içeriği "Firmamızda, önemli bilgilerin gizliliğinin korunabilmesi için Güvenli belge deposu'na benzer önlemler bulunur" olduğundan dolayı Faktör 1 "Gizlilik"; Faktör II'de en fazla faktör

yük değerine sahip olan madde 10 olup içeriği "Ciddi bir siber saldırı ile bilgilerimizin zarar görmesi durumunda firmamızın önemli derecede etkileneceğini düşünmekteyim." olduğundan dolayı bu faktör "Bütünlük-Tamlık"; Faktör III'de ise en büyük faktör yük değerine sahip olan madde 34'ün içeriği "Firmamız, müşterilerimizin bilgilerini başka kurumlarla paylaşmadan önce ilgili kişiye bilgi verir" olduğundan dolayı "Mahremiyet"; Faktör IV'de de en büyük faktör yük değerine sahip olan madde 12'nin içeriği "Kullandığımız bilişim sistemlerinin herhangi bir unsurunun (yazılım veya donanım vb.) kendisinden beklenildiği şekilde çalışmaması işlerimizi önemli ölçüde yavaşlatır" ifadesinden oluştuğundan dolayı "Kullanılabilirlik ve Süreklilik" olarak isimlendirilmiştir. Faktörlerin isimlendirilmesi ve içerdikleri madde sayısı Tablo 11'de verilmiştir.

Tablo 11. Faktörler ve İçerdikleri Madde Sayıları

Faktörler	İsimleri	İçerdikleri Madde sayıları
Faktör 1	Gizlilik	15
Faktör 2	Bütünlük	8
Faktör 3	Mahremiyet	6
Faktör 4	Erişebilirlik	4

Araştırmaya esas aldığımız ve Cherdantseva, Rana, Ivins, & Hilton (2013) tarafından geliştirilen "RMIAS" modeli, araştırmanın modeli olarak kullanılmıştır. Bu araştırma modeli sekiz bölümden oluşmaktadır. Ancak araştırmada kullanılan ölçeğe Faktör analizinin uygulanması sonucunda ölçekteki maddelerin dört factor altında toplandığı tespit edilmiştir: Gizlilik, Bütünlük-Tamlık, Erişebilirlik ve Mahremiyet. Orijnallik-Güvenirlilik ile ilgili maddelerin "Gizlilik" adını verdiğimiz faktör yüklenmiştir. Bunun nedeni literatürde Orijnallik güvenirlilik Başka bir deyişle, kimlik doğrulama bilgisayar sistemine giriş yapan kişinin iddia edilen kişi olup olmadığını doğrulamaktadır (Karsten, 2011). Bu noktada tanımların birbirine yakın olmasından dolayı katılımcılar Orjinallik ve güverliliği Gizlilik ile aynı faktör olarak algılamış olabilecekleri ifade edilebilir.

Gizlilik faktörünün altında toplanan bir başka faktör ise İzlenebilirilik'tir. Alan Westin (1967) tarafından gizliliğin tanımı; bireylerin kendileriyle ilgili kişisel bilgilerin başkalarına iletilmesiyle ilgili sahip oldukları haklar olarak tanımlanmaktadır ve bu tanım izlenebilirliğin temelini oluşturmaktadır. Westin (1967) gizliliği bütün bilgileri kapsayacak şekilde açıklamıştır ve bundan dolayı da katılımcıların İzlenebilrililik ile ilgili maddeleri gizlilik maddeleri olarak algıladıkları ifade edilebilir.

Gizlilik fatktörünün altında toplanan bir başka faktör ise denetlenebilirililik'tir. Denetlenebilirlilik literatürde "veritabanındaki öğelere erişen (veya değiştiren) kişileri takip edebilme eylemi" (Fariborz Farahmand, Sharp, & Enslow, 2005) ve gizlilikte yetkisi olmayan kişilerin girişlerinin engelenmesi olarak tanımlanmıştır. Bu nedenle katılımcıların izinsiz girişlerin engelenmesini, denetlenebirlilik olarak algılamış olabilecekleri söylenebilir.

İkinci faktörün Bütünlük-Tamlık başlığı altında toplandığı görülmektedir. İnkar edememeyle ilgili maddeler bu başlık altında toplanmıştır. Literatürde Tamlık-Bütünlük veri bütünlüğü, istenmeden bilginin değiştirilmemesi ya da zarar görmemesi olarak tanımlanmaktadır (Knorr, Rohrig, 2015). İnkar edememe ise bir davada tarafları diğer tarafa karşı korumak ve belirli bir eylemin veriler üzerinden değişiklik yapılmadan eylemin gerçekleşip gerçekleşmediğini kanıtlamak için önemli veriler olarak tanımlanmaktadır (Zhou ve Gollmann, 1997). Bu yüzden katılımcılar inkar edememe ile ilgili verileri Tamlık-Bütünlük olarak algılamış olabilecekleri ifade edilebilir.

4. BULGULAR VE YORUMLAR

Araştırmaya katılanların cinsiyetleri incelendiğinde %57'sinin erkek % 43'nün ise kadın olduğu tespit edilmiştir.

Araştırmaya katılanların gelir düzeyleri incelendiğinde, %41,1'i 2000 TL ve altı bir gelire sahip olduğunu; %32,5'i 2001-4000 TL arasında; %14,3'ü 4001-5000 TL arasında; %8,1'i 5001-7000 TL arasında; %4'ü ise 7001 TL ve üzeri bir gelire sahip oldukları belirlenmiştir.

Katılımcıların yaş aralığı incelendiğinde, 262'sı 20-25 yaş aralığında; 201'i 26-30 yaş aralığında; 145'i 31-35 yaş aralığında; 72'si 36-40 yaş aralığında; 54'ü 41-45 yaş aralığında; 18', 46-51 yaş aralığında; 4'ü ise 52 ve üzeri olduğu görülmektedir.

, ilköğretim düzeyinde mezun olanların 33 kişi; Lise mezunları 129 kişi; Önlisans mezunları 185 kişi; Lisans mezunları 346 kişi; lisansüstü mezunlarının 63 kişi olduğu belirlenmiştir

Katılımcıların çalıştığı kurumdaki pozisyonları incelendiğinde, üst düzey yönetici olarak 83 kişi ile %11, orta düzey yönetici grubunda 134 kişi ile %17,7, alt düzey yönetici grubunda 167 kişi ile %22.1, teknik çalışan pozisyonunda 128 kişi ile %16,9, idari çalışan kısmında 244 kişi ile %32,3 olduğu görülmektedir

Kurumların faaliyet yılları incelendiğide ise, kuruluşu 0-5 yıl içerisinde olan 125 firma (%16,5) olduğu, 6-10 yıl arasında 196 firma (%25,9) olduğu, 11-15 yıl arasında 136 firma (%18) olduğu, 120 firmanın (%15,9) 16-20 yıl içerisinde kurulduğu ve 21 yıl ve üzerinde ise 179 firmanın (%23,7) olduğu görülmektedir

5. SONUÇ

Globallaleşen dünya ile birlikte, iletişim teknolojisinde yaşanan gelişmeler, firmalar için sınırları ortadan kaldırmıştır. Yaşanan bu dönüşüm, Sadece firmalar için değil, insanlığın her alanında değişime neden olmuştur.

İnternet ve bilişim teknolojileri, otomasyon, yapay zeka, internet ve yeni iş modelleri insan hayatının her alanı etkilemektedir. Teknolojiyle birlikte insanlar, oturdukları yerden istedikleri alışverişi yapmakta ve istediği bilgiye ulaşabilmektedir. İş dünyası hem üretim metotlarında ve ürün geliştirmede, hem de hizmet sunum süreçlerinde yeni dinamikler geliştirmektedir. Sağladığı avantaj ve getirdiği tehditlerle yaşadığımız yüzyıl, şirketler açısından büyük kolaylıklarla birlikte büyük sorunları da beraberinde getirmektedir.

Teknolojide yaşanan değişim, şüphesiz insanlık hayatına kolaylıklar getirmektedir. Bununla birlikte bu yenilikler, yeni tehditleri de berbarinde getirmekte ve sonuçta "Bilgi Güvenliği" kavramı dünyada yeni bir gündem olarak ortaya çıkmaktadır. Dünya, dijitalleşmeyle birlikte, pazarlama, satış, üretim, vergi gibi kavramları yeniden tanımlarken risk ve tehditleri de yeniden tanımlar hale gelmiştir. Daha önceden, hangi nedenlerle ve kaynağı tahmin edilebilecek risk ve tehditler konuşulurken, günümüzde tehditlerin nereden geleceği tahmin edilememektedir. Günümüzde sadece şirketler değil, kamu kurumları ve ülke güvenliği de tehdit altındadır.

Daha önceki bölümlerde bahsi geçen ve 2001 yılında ortaya çıkan Codered solucanı, 2003 yılında ortaya çıkan Blaster solucanı, 2013 Target firmasına yapılan saldırı ve Türkiye'de 2015 yılında yapılan siber saldırı sonucunda oluşan elektirik kesintisi, üreticileri ve kamu kurumlarını çalışamaz hale getirmiştir.

Teknolojide yaşanan gelişim ile birlikte siber saldırı teknikleri aynı gelişim hızıyla kendini ilerletmektedir. Bununla birlikte, operasyon süreçlerinin zarar görmesi, maddi kayıplar, rekabet gücünde yaşanacak sorunlar ciddi itibar ve güven kaybına ve sonuçta firmalar için telafisi zor kayıplara neden olabilmektedir. Firmalar dijital gelişimin sağladığı fırsatlardan

hız kesmeden yararlanması ama aynı zamanda gelebilecek olan tehditlere hazırlıklı olması gerekmektedir.

Dünya hızla dönüştüğü zaman herşey daha hızlı bir şekilde değişmektedir. Teknolojideki gelişime uyum göstermek, fırsatlardan yararlanabilmek, gelebilecek siber saldırılara karşı bilgi ve öngörüye ve gerekli adımları atabilecek esnekliğe sahip olmak firmalar için önemlidir.

Bütün bunlar sonucunda, bu çalışmanın amacı, Kobi'lerin bilgi güvenliği farkındalıklarını ölçebilmek için güvenilir ve geçerli bir ölçek geliştirmektir. Ölçeğin boyutlarının belirlenmesini belki ölçek geliştirmedeki en zor kısımdır. Bu amaçla literature araştırmasının yanında, faktör analizi yapılmıştır.

Sonuçlar, 37 maddenin ''Kobilerin Bilgi Güvenliği Farkındalığı Ölçeğini' ölçtüğünü göstermektedir. Sonuçlar, ölçeğin 8 boyutlu olduğunu göstermiştir. Sonuçlara göre alt ölçekler;

i. Süreklilik
ii. İzlenebilirlik ya da Kayıt Tutma
iii. Kimlik Sınaması
iv. Bilginin Erişebilirliği
v. Bilgi Bütünlüğü
vi. Gizlilik
vii. İnkar Edememe
viii. Mahremiyet

Ölçüt geçerliliğini ispatlamak için Hemzaman/Eşzaman geçerliliği yöntemi kullanılmıştır. 2014 yılında Akademisyenler üzerinde Bilgi güvenliği farkındalığı ölçeği (ABGFÖ) ile Bilgi güvenliği farkındalığı ölçeği aynı anda uygulanmış ve elde edilen sonuçlar arasında korelasyona bakılmıştır. Koreleason değeri r = 0,407 olup istatistiksel olarak anlamlıdır ($p=0,003<0,05$). Elde edilen bu korelasyon değerine göre geliştirilen ölçek ile daha önceki ölçek arasında pozitif yönde ve orta düzeyde bir ilişki olduğu tespit edilmiştir.

Yapı geçerliliğini ispatlamak için Açımlayıcı Faktör analizi ve Doğrulayıcı faktör analizi yapılmıştır. Faktör analizlerinin farklı örneklem gruplarından elde edilen veriler üzerinden yapılması gerektiği ifade edildiğinden, geçerli sayılan 756 ölçek formu rastgele ikiye bölünerek AFA ve DFA uygulanmıştır. (n1=378; n2:378) ilk grup üzerinde AFA, diğer grup zerinde DFA yapılmıştır.

Açımlayıcı faktör analizi sonuçları, örneklem büyüklüğü yeterliliği için KMO test edilmiş ve çıkan sonucun 0,942 olduğu tespit edilmiş ve örneklem büyükllüğünün yeterli olduğunu göstermiştir. Madde analiz sürecinde ''0,40'' altında çıkan 4 maddenin (S2, S14, S17 VE S18), ölçekten çıkarılması kararına varılmıştır. Sonuçlara göre temel bileşenler yöntemi ve dik döndürme sonunda faktör özdeğerleri ve faktörlerin toplam varyansı %67,33'nü açıkladığı göstermiştir. Çıkan bu sonuç ölçeğin faktör yapısının güçlülüğüne işaret etmektedir. Faktör sayısını belirleme için çizgi grafiği incelenmiş olup, ölçeğin içerdiği anlamlı faktör sayısının dört olduğunu göstermiştir. Faktörlerin içindeki maddelere bakıldığında en fazla maddeye sahip olan faktör, faktör adları olarak kullanılmıştır. Bunun sonucunda, Faktör 1 Gizlilik, Faktör 2 Bütünlük, Faktör 3 Mahremiyet, Faktör 4 Erişebilirlik olarak adlandırılmıştır. Ölçeğin dört farktörde çıkma nedeni, Literatürde daha önce belirtildiği üzere bilgi güvenliğinin temelini CIA Bütünlük, Gizlilik ve Erişebilirlik oluşturuyodu. Çıkan faktörlere baktığımızda Mahremiyet harcicinde diğer faktörler CIA modelini oluşturmaktadır.

Doğrulayıcı faktör analizi için, Ki kare uyum iyiliği indeksi ile birlikte, Artırmalı Uyum İndeksi (Incremental Fit lndex, IFI), Karşılaştırmalı Uyum İndeksi (Comparative Fit Index,

CFI), Yaklaşık Hataların Ortalama Karekökü (Root Mean Square Error of Approximation, RMSEA), İyilik Uyum İndeksi (Goodness Of Fit Index, GFI), Ortalama Hataların (Kalıntıların) Karekökü (Root Mean Square Residual, RMR) bakılmıştır. Modele ait $\boldsymbol{\chi^2/df}$ değerinin 1,937 olduğu görülmektedir $\boldsymbol{\chi^2} = 943{,}216\ ve\ df = 487$) bu değer 3'den küçük olduğu için modelin uyumu iyi olarak yorumlanabilir. Benzer şekilde IFI ve RMSEA değerleri sırasıyla 0,951 (≥0,95) ve 0,050 (≥0,050) olarak hesaplanmıştır. Hesaplanan her iki uyum indeks değeri için modelin uyumu iyi olarak kabul edilmektedir. Diğer uyum değerleri olan GFI, CFI ve RMR değerleride sırasıyla 0,863(≥0,85), 0,950 (≥0,95) ve 0,055 (0<RMR<0,08) olarak tespit edilmiştir. Bu üç uyum değerine gore, elde edilen modelin kabul edilebilir uyum değerlerine sahip olduğunu ortaya koymaktadır.

KBGFÖ'nin güvenirliği için iç tutarlılık Cronboach Alpha yöntemi ile hesaplanmıştır. . KBGFÖ ölçeğinin genel güvenirliği 0,954, Birinci faktörün 0,947, ikinci faktörün 0,927, üçüncü faktörün 0,923 ve dördüncü faktörün 0,924 olduğu tespit edilmiştir. Bu değerler dikkate alındığında ölçeğin oldukça güvenilir olduğu sonucuna varılmıştır.

6. ÖNERİLER

Günümüzde, Bilgi güvenliği firmalar için çok önemli olması nedeni ile, bu ölçek firmaların bilgi güvenliği farkındalıklarını ölçülmesi için çok önemli katkıları olabilir. Firmalar bilgi güvenliği farkıdalıklarıyla ilgili güçlü ve zayıf olduğu noktaları görebilir ve gereken önlemleri alabilirler.

Gaziantep sınırları içerisinde kobilerin bilgi güvenliği farkındalıklarını ölçmeye yönelik geliştirilen ölçek kullanılarak, gelecek araştırmalar için çeşitli öneriler belirtilebilir. Bu konuda yapılan araştırmaların kobilerin bilgi güvenliği alanında literatürdeki boşluğun doldurulmasına katkıda bulunacağı düşünülmektedir..

Yapılan araştırmalar sonucunda geliştirilen 'kobilerin bilgi güvenliği farkındalığı ölçeği' kullanılarak farklı coğrafyalarda farklılıklar/benzerlikler ortaya konularak kuramsal tartışmalara katkı sağlamak amacıyla yeni araştırmalar yapılmalıdır.

Kobilerin bilgi güvenliği farkındalıklarıyla ilgili zayıf olduğu noktaların tespit edilmesi sonucunda bu zayıf noktaların giderilebilmesi için yeni araştırmalar, farklı örneklem grupları üzerinde yapılmalı, böylece sorunların çözümü için öneriler sunulmalıdır.

Araştırma, Gaziantep sınırları içerisinde kobiler üzerinde gerçekleşmiştir. Daha sonraki araştırmaların daha büyük örneklemlerde gerçekleştirilerek, sonuçların karşılaştırılması ile alan yazına katkıda bulunulması önerilmektedi

KAYNAKÇA

AdaletBakanlığı.(2012).http://www.ankara.adalet.gov.tr/duyurular/dosyalar/2015/10/EK2.pdf (12.10.2017).

Aytaç, M., ve Öngen, B. (2010). Doğrulayıcı faktör analizi ile yeni çevresel paradigma ölçeğinin yapı geçerliliğinin incelenmesi. İstatikçiler Dergisi. 5,14-22.

Aydın, K. Ve Yayla, H. E. (2018). Muhasebe meslek mensuplarının etik tutumlarının kurumsalitibar yönetimi üzerindeki etkisi1. Atlas International Referred Journal On Social Sciences. 4, (8). 67-97.

Bisson, D. (2015). The OPM breach: Timeline of a hack, Tripwire 1-8.

Boateng, Y. ve Osei, E. (2013). Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity and Availability (CIA). Doktora tezi, Aalborg University, Aalborg: 185-187

Büyüköztürk, Ş. (2002). Faktör analizi: Temel kavramlar ve ölçek geliştirmede kulanımı. Kuram ve Uygulmada Eğitimi Yönetimi. Dergipark Sayı:32:470-483

Cherdantseva, Y. ve Hilton, J. (2013). A Reference Model of Information Assurance and Security ARES 2013 secont workshop 2-6. Regensburg:Germany University of Regensburg IEEE. 57-50.

Cherdantseva, Y., Rana, O. Ivins, W. ve Hilton, J. (2016). A Multifaceted Evaluation of the Reference model of information assurance and security. ScienceDirect,Computer&Security. 63, 45-66:

CNSS. (2010). Committee on national security systems. National Information Assurance (IA) Glossary . Instruction No. 4009.

Fariborz Farahmand, Sharp, G., ve Enslow, P. (2005). A management perspective on risk of security threats to ınformation systems. Springer Science. 6(2-3), 203-225.

Hpe Security Reseacrh (2016). Cyber risk report 2016. California: 57

Karasar, N. (1995). Bilimsel araştırma yöntemi. 7.basım Sim Matbaası. Ankara:62

Karsten, B. (2011). Authentıcatıon and securıty aspects in an international multi-user network. 5.

Knorr, K. ve Rohrig, S. (2015). Security requirements of e-business processes. Zürih: University Of Zurich.

Maconanchy, W., Schou, C., Ragdale, D., ve Welch, D. (2001). A model for ınformation assurance: An ıntegrated approach. 2001 IEEEE Workshop on Information Assurance and Security. NY: U.S Military Academy.

McCumber, J. (1991). Information systems security: A compre- hensive model. Baltimore 14th National Com- puter Security Conference.

Pearson, S. (2012). Privacy Management in Global Organisations. https://link.springer.com/conference/cms 217-237(12.10.2017)

Polit, H. ve Portney, W. (1993)Research in health care:concepts designs and methods 2th Edition:112

Saltzer, J., ve Schroeder, M. (1975). The protection of information in computer systems. Procedings of the IEEE Volume:63 Issue:9:1278-1308

Sorrentino, F., (2015) Cyber Attacks: 5 Ways Small Businesses Can Protect Themselveshttps://www.forbes.com/sites/franksorrentino/2015/10/26/cyber-attacks-5-ways-small-businesses-can-protect-themselves/#2a17abe53193. (5.02.2016).

Tavşancıl, E. (2002). Tutumların ölçülmesi ve SPSS ile veri analizi. Ankara: Nobel Yayınevi.

Tezbaşaran, A. (1996). Likert tipi ölçek gelştirme kılavuzu. Ankara: 2.baskı Psikoloji Derneği Yayınları.

Weitzner, D., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J. ve Sussman, G. (2008). Information accountability. Communications of the ACM. 83

Westin, A. (1967). Privacy and freedom. Atheneum, New york.

Whitman, M. ve Mattord, H. (2014). Principles of ınformation security. Fourth Edition Course Techonology, Cengage Learning:32

Wilson M. Hash J. (2003). Computer security, national ınstitute of standards and techonology Nist Special Edition 800-50, Washington: 9.

Yıldız, M. (2014). Siber suçlar ve kurum güvenliği. Ankara: Ulaştırma Denizcilik ve Haberleşme Bakanlığı Bilgi İşlem Daire Başkanlığı. Denizcilik uzmanlık tezi 58-59

Zhou, J. ve Gollmann, D. (1997). Elsevier. Journal of Network and Computer Applications. 20(3), 267-281.