GÜVENLİK GÜÇLERİNİN BİLGİ GÜVENLİĞİ FARKINDALIĞINI BELİRLEMEYE YÖNELİK BİR ARAŞTIRMA[*]

Emre TANER[**], İbrahim KILIÇ[***]

Öz

Bu araştırmanın amacı, emniyet ve asayiş ile kamu düzenini korumakla görevli olan emniyet personelinin bilgi güvenliği farkındalık düzeylerinin tespit edilmesidir. Çalışmaya, Siirt'te görev yapan 207 jandarma ve 197 polis olmak üzere toplam 404 personel katılmıştır. Veri toplama aracı olarak anket kullanılmıştır. Verilerin analizinde, betimsel istatistiklerin (frekans, yüzde, ortalama, standart sapma) yanı sıra, bilgi güvenliği farkındalık düzeylerinin katılımcıların demografik özelliklerine göre karşılaştırılmasında t testi ve varyans analizi kullanılmıştır. Araştırma sonucunda, bilgi güvenliği farkındalık düzeyi ölçeğinin "saldırı ve tehditler" alt boyutuna ilişkin genel ortalama 2,32 ve "kişisel verileri koruma" alt boyutuna ilişkin genel ortalama ise 2,87 olarak hesaplanmıştır. Bu değerler emniyet personelinin bilgi güvenliği farkındalık düzeylerinin yüksek olmadığını hatta ortalamanın altında olduğunu göstermektedir. Diğer taraftan katılımcıların bilgi güvenliği farkındalık düzeylerinin bazı demografik özellik değişkenlerine göre farklılık gösterdiği tespit edilmiştir. Araştırma sonuçları, emniyet personelinin bilgi güvenliği farkındalık düzeylerinin artırılmasına yönelik önlem alınmasını ve gerekli çalışmalar yapılmasını ortaya koymuştur. Bununla birlikte konu ile ilgili farklı çalışmaların farklı illerde farklı örneklemlerle yapılması bilgi güvenliği farkındalık düzeyinin mevcut durumunu betimleyecek, literatüre önemli katkılar ve ilgili birimlerin önlem alması konusunda yöneticilere önemli veri kaynağı oluşturacaktır.

Anahtar Kelimeler: *Bilgi, Bilgi Güvenliği Farkındalığı, Kişisel Bilgilerin Korunması, Güvenlik Personeli*

A STUDY ON DETERMINING INFORMATION SECURITY AWARENESS OF SECURITY FORCES

Abstract

The aim of this study was to determine the information security awareness levels of the security forces responsible for protecting public order and security. A total of 404 personnel participated in the study, including 207 gendarme and 197 policemen working in Siirt province of Turkey. Questionnaire was used as data collection technique. In the analysis of the data, in addition to descriptive statistics (frequency, percentage, mean, standard deviation), t test and variance analysis were used to compare the information security awareness levels of the security forces according to the demographic characteristics of the participants. According to the results of the study, the overall average regarding the "attack and threats" sub-dimension of the awareness levels of information security was calculated as 2.32 and the overall average for the "personal data protection" sub-dimension was calculated as 2.87. These values indicated that the information security awareness levels of the safety personnel were below the average. On the other hand, it was determined that the participants' awareness levels of information security varied according to some demographic characteristics. According to the results of the study, it was suggested that precautions should be taken to increase the awareness levels of the safety personnel about the information security and it has been revealed that studies should be carried out to increase the information security awareness levels of security forces. Furthermore, conducting different studies in different sample groups in different provinces will describe the current level of information security awareness level, make important contributions to the literature and provide important data for the managers to take precautions for the relevant units.

Keywords: *Information, Information Security Awareness, Protection of Personal Information, Security Personal*

---

[*] Bu araştırma yazar Emre TANER'in yüksek lisans tezinden üretilmiştir.

[**] Afyon Kocatepe Üniversitesi, Fen Bilimleri Enstitüsü, İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı, emretaner32@gmail.com, ORCID ID: https://orcid.org/0000-0002-8092-9308

[***] Doç. Dr., Afyon Kocatepe Üniversitesi, Biyoistatistik Anabilim Dalı, Türkiye, kilicibrahim@hotmail.com, ORCID ID: https://orcid.org/0000-0003-0595-8771

Makale Geliş Tarihi: 31.05.2019 Makale Kabul Tarihi: 15.08.2019

GİRİŞ

Bilgi; insanoğlunun var olmasından itibaren düşüncesini, davranışını ve gelişim sürecini belirleyen en önemli faktörlerden biridir (Vural, 2007). Tarih boyunca insanoğlunun sahip olduğu en önemli olgu olmasından dolayı bilgi kavramı aynı zamanda güç olarak algılanmaktadır (Güçlü ve Sotirofski, 2006). Bilgi konusuna sosyolojik açıdan yaklaşan Aydın (2004) bilgiyi insanın kendini anlama ve yorumlayabilme biçimi olarak tanımlamaktadır. Irzık (2002) bir şeyin bilgi olabilmesi için doğru olması gerektiğinin öne sürmüştür. Özellikle teknoloji çağında görsel medya yoluyla alınan bilginin ne kadar doğru olacağı ve toplum yararına olan katkısını sorgulamıştır. Burada bilginin toplum ihtiyaçlarını ne denli karşıladığını ve toplum yararına ne denli katkıda bulunduğunun sorgulanması gerektiğine değinilmiştir.

Bilgi tek başına bir unsur olmasının yanında birçok değerin birleşmesi sonucu oluşmuştur. Bilgi, davranış, kapasite ve enformasyon unsurunun birleşmesiyle meydana gelmiştir. Yani kısacası bilgi deneyim, kültür, huy, algılama ölçüsü, bakış açısı, kişilik gibi birçok faktörün bir araya gelmesi ile oluşmuştur (Türk, 2003). Mengüşoğlu (1988), bilginin nitelikleri üzerine yapmış olduğu incelemede bilgiyi; bilimsel bilgi, doğal bilgi, felsefi bilgi, sanatsal bilgi ve din bilgisi olmak üzere 5 temel tür üzerinde sınıflandırmıştır. Genel olarak kabul edilen bu türlere Aydın (2004), teknik ve politik bilgiyi de ekleyerek 7 temel tür altında toplamıştır. Yeniçeri ve İnce (2005), bilgiyi kullanım alanı, kaynağı, rekabet üstünlüğü ve niteliğine göre 4 ana unsurda birleştirmiş ve farklı türlere ayırmıştır.

Bilginin anlamlı bir sonuca ulaşılabilmesi için onu oluşturan bazı unsurlar vardır. Konunun uzmanlarınca yapılan çalışmalar sonucunda bu unsurlar veri ve enformasyon olarak karşımıza çıkmaktadır. Bu iki kavram bilginin oluşmasında ve kaybolmasında etkin rol oynayan unsurlardır. Bu unsurlar birbirleri ile doğrudan ilişkilidirler. Bilgi kişisel bir oluşumdur. Bir kişiden diğerine doğrudan iletilmesi mümkün değildir. Bundan dolayı bilgiyi oluşturan temel unsurlarda en az bilgi kadar önem arz etmektedir. Türkçemizde günlük kullanım dilinde bilgi, veri ve enformasyon kavramları çokça birbirine karıştırılmaktadır. Bu kavramlar arasındaki anlam farklılıklarını doğru ayırabilmek, kavramları sahip oldukları gerçek anlamları ile tanımlayabilmek doğru kullanım ve bilgiye ulaşmak açısından oldukça önemlidir (Odabaş, 2003; Yılmaz, 2009; Demirtaş, 2013).

Bilginin zaman içerisindeki yoğun artışı ve teknolojinin gelişmesi ile birlikte var olan bilgilerin elektronik ortamlara taşınması gereği doğmuştur. Çok fonksiyonlu, boyut olarak çok az yer kaplayan büyük teknolojik cihazlar sayesinde daha fazla bilgi dijital ortama aktarılmakta, işlenmekte ve taşınabilmektedir. Tüm bu teknolojik gelişmeler bireylerin günlük yaşantısında iletişim kurma ve bilgi paylaşmada sağladığı hız ve kolay erişilebilirlik vb. avantajları sebebiyle tercih edilmektedir (Erdoğmuş, 2017). Ancak bu avantajların kullanılabilmesi için

kişilerin, sürekli gelişen ve daha karmaşık bir hal alan teknolojik gelişmeleri yakından takip etmesi gerekmekte ve iletişim için gerekli akıllı cihazları ve içerdiği yazılımları kullanmak için gerekli teknolojik bilgiye sahip olması gerekmektedir. Yani bilgi ve iletişim için sadece okuma yazma bilgisi yetmemekte, bunun yanında bireylerin gerekli medya okur-yazarlığını da bilmesi gerekmektedir (Mart, 2012).

Bilgi teknolojilerinin, bilgi kaynaklarına hızlı ulaşım sağlaması, ulaşılan bilginin hızlı bir şekilde aktarımı, sosyalleşme, çevrimiçi anlık iletişim kurma gibi faydalarının olmasının yanında birçok olumsuzluğu da beraberinde getirmektedir. Sanal ortamlarda bilgiye ulaşmanın kolay olması kadar zararlı içeriklere de erişimin kolay olması ve bu içeriklere daha fazla maruz kalınması bireylerin sosyal yaşantılarında olumsuz etkilere sebep olmaktadır.

Gerçek dünyadan farklı olan bu dijital dünyada kişiler arası ilişkiler değişmekte ve gerçek dünyada iletişim kurmada önemli olan yaş, cinsiyet, ırk, kültür vb. pek çok özellik sanal dünyada önemli olmamaktadır. Online alışveriş, bankacılık faaliyetleri, hatta doğrudan internet üzerinden çalışma vb. kullanımlar insanın sosyal yaşamını etkileyecek unsurlardır (Ertuğrul ve Keskin, 2012). Bu süreçte en önemli unsur, internet ve sanal dünya bakımından bilgi güvenliğidir.

Yukarıdaki bilgiler çerçevesinde bu çalışmada, emniyet ve asayiş ile kamu düzenini korumakla görevli olan, toplum huzuru ve ülke menfaatleri çerçevesinde suç önleyici çalışma yürüten ve bu çalışmaları yürütürken birçok gizli bilgiyi de bünyesinde barındıran güvenlik (polis, jandarma) personelinin bilgi güvenliği farkındalık düzeylerinin tespit edilmesi amaçlanmıştır.

1. BİLGİ GÜVENLİĞİ

İnternetin hayatın her alanına nüfuz etmesi günümüzde, banka bilgileri, çalışma hayatıyla ilgili bilgiler, kişinin yaşantısını ilgilendiren tüm unsurlar, kısacası tüm kişisel veriler yeni nesil akıllı teknolojik cihazlar ile saklanmakta ve internet yardımı ile istenildiği zaman istenildiği yerde ulaşılmakta ve başka bir alıcıya gönderilmesini mümkün kılmaktadır (Çetin, 2014). Yeni nesil akıllı cihazlar ve beraberinde geliştirilen tüm yardımcı uygulamalar hayatımızı kolaylaştırmasının yanında bazı güvenlik problemlerini ve yeni suçları da beraberinde getirmektedir (Gülmüş, 2010). Özellikle mobil cihazlardaki gelişim ve akıllı telefonların hayatımıza girmesi ile birlikte internet, sosyal medya programları, bankacılık faaliyetleri vb. bilgisayar üzerinden yapılan birçok işlem cep telefonlarından yapılabilir olması internet kullanımında da artışa sebep olmakta ve artık mobil internete kullanımına doğru bir eğilimin olduğu görülmektedir (Bolat, Aydemir ve Karaman, 2017).

İnternet ve çevrimiçi dünyanın hayatımızı giderek kuşatması ile birlikte kötü niyetli bilgisayar korsanları tarafından bir hedef haline gelmiş ve siber saldırı sayısı artmıştır. Bu durum sahip olunan bilginin korunmasını da sorun haline getirmiştir

(Karaaslan, 2013). Özellikle kritik sayılacak kurumlarda görev yapan personele ait kişisel verilerle personelin iş yaşantısı ile alakalı elektronik ortamlarda tuttuğu kayıtlara kötü niyetli kişilerce erişilmesi, kurumun güvenliğini de tehlikeye atacağından, kişisel veri güvenliğinin kurumsal veri güvenliğini de etkilemesi söz konusu olacaktır.

21. yüzyılın bilgi çağı olmasından dolayı, şirketler, devlet kurumları, sağlık, eğitim vb. tüm alanların ortak paydası bilgi çağında yaşıyor olmalarıdır. Bu kurumlar arasında ister üretim alanında ister tüketim tarafında ve ister hizmet alanında bulunan sahip olunan en önemli değer bilgidir. Kurumların veya şirketlerin birbirleriyle rekabet edebilmesi ve gerçekleştireceği her türlü faaliyetlerinde bilgi unsuru kesinlikle yer alacaktır. Bu durum sahip olunan bilginin önemini de artırmaktadır. Bu kadar değerli ve vazgeçilmez olan bilginin uygun bir şekilde korunması da başlı başına bir iş ve alan olmuştur (Eminağaoğlu ve Gökşen, 2009).

Bilgi çağı ve toplumunda yaşayan bireyler, şirketler ve kurumlar olarak bilgi güvenliği konusu sadece belli bir kesimin konusu olmaktan çıkmış ve bilgiye sahip olan herkesi ilgilendiren bir konu haline gelmiştir. Schmidt (2004)'e göre bilgi güvenliği kavramı, bilgiye istenildiği zaman erişilme imkânı olan elektronik platformlarda, bilginin gönderici ve alıcı arasındaki transfer sürecinde, bütünlüğünün sağlanması ve üçüncü şahısların nüfuz etmeden güvenli bir şekilde gönderilmesi şeklinde tanımlanmıştır (Yılmaz, Şahin ve Akbulut, 2016). Kısacası bilgi güvenliği, elektronik ortamlarda bilgilerin depolanması ve iletimi esnasında bilgilerin içeriğinin bozulmadan, yetkisiz kişilerin erişiminden korunması için güvenli bir alan yaratma çalışmalarının tümü olarak tanımlanmaktadır (Canbek ve Sağıroğlu, 2006).

Sayarı (2009)'ya göre elektronik ortamlarda tutulan bilginin güvenliğinin sağlanamaması durumunda; kurumların sahip oldukları ve özellikle gizli içerikli bilgiler üçüncü şahısların eline geçebilecek, sahip olduğu bilgiyi koruyamayan ve üçüncü şahısların eline geçmesini önleyemeyen kurumlar ciddi itibar kayıpları yaşayacak, kamu kurumlarında kaybedilen hassa bilgiler ülke menfaatlerine zarar verebilecek, bilginin kaybedilmesi onu tekrar sağlayabilmek için belli bir süre iş ve zaman kaybına yol açacak ve özellikle kamusal anlamda ve bazı önemli kurumlar yasal olarak ciddi yaptırımlara maruz kalabilecektir.

Bilgi güvenliğinin sağlanması konusunda korunacak bilgi varlıklarının seçilmesi, sınıflandırılması ve uygun güvenlik önlemlerinin tespit edilmesi gibi işlemleri en önemli hususlardan biri olmasına rağmen, bu konunun çoğu zaman dikkate alınmadığı bilinmektedir (Henkoğlu, 2017). Bilgi güvenliği risklerinden korunmak için kurumsal seviyede her ne kadar yüksek miktarda paralar harcansa da halen güvenlik seviyesi %100'lere ulaşamamaktadır. Bunun başlıca sebeplerinden biri, kurumlarda bulunan bu bilgi teknolojisi ürünleri kullanan insan

faktöründen kaynaklanmaktadır. İnsan kaynaklı bilgi güvenliği ihmallerini ve doğuracağı riskleri %0 seviyelerine indirmek imkânsız gibi görünse bile profesyonel bir ekip tarafından hazırlanmış farkındalık eğitimleri ile bilgi güvenliği zafiyetleri minimum seviyeye indirilebilir. Görüldüğü üzere bireylerde, bilişim teknolojileri alanında yapacağı tüm işlemlerde bilgi güvenliği farkındalığının oluşması gerek kişisel gerekse kurumsal, alanda önem arz etmektedir. Bir kurumun bilgi güvenliği seviyesi o kurumda çalışan bireylerin bilgi güvenliği farkındalık seviyesi ile doğrudan ilişkilidir (Vural, 2007; Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009; Gülmüş, 2010).

Teknolojik gelişmelerle birlikte son yıllarda bilgi güvenliği konusuna olan ilgi tüm dünyada ve ülkemizde oldukça artmıştır. Bu konuda yapılan araştırmaların çoğu teknik altyapı ile ilgili olan; güvenlik duvarı, IP analizi, saldırı tespit/önleme sistemleri, anti virüs yazılımları, şifreleme programları, kimlik doğrulama, yetkilendirme vb. konularla ilgilidir. Oysaki insan faktörünü göz ardı eden tüm bu çalışmalar tek başına yeterli olmamaktadır. Bir kurumda bilgi güvenliği konusu, teknik önlemlerin alınmasının yanında çalışanlarının da güvenlik bilincine ulaşması ile birlikte sağlanabilir (Keser ve Güldüren, 2015).

Bilgi güvenliğine yönelik son yıllarda ülkemizde pek çok bilimsel çalışma yapılmıştır. Yılmaz ve Ezin (2017), ebeveynlerin bilgi güvenliği farkındalıklarının incelenmesi üzerine yapmış oldukları çalışma neticesinde ebeveynlerin belli bir seviyede bilgi güvenliği farkındalığı olduğu fakat bazı spesifik (depolama yerleri, depolama süreleri vb.) konularda farkındalık seviyelerinin yetersiz olduğu sonucuna varmıştır. Ayrıca ebeveynlerin çocuklarına bilgi güvenliği konusunda uyarıdan başka somut bir bilgi veremedikleri sonucuna ulaşmışlardır. Çek (2017), kurumsal bilgi güvenliği ve bilgi güvenliğinde insan faktörünün önemi ile ilgili yapmış olduğu yüksek lisans tezinde bilgi ve bilgi güvenliğiyle ilgili çeşitli kavramları açıklayarak kişisel boyutta bilgi güvenliğinin önemi ve bilgi güvenliğinin sağlanması için alınabilecek önlemleri sıralamıştır. Erdoğmuş (2017), üniversite öğrencilerinin bilgi güvenliği kazanımlarının farkındalıkları üzerindeki etkilerini belirlemek amacıyla bir anket çalışması yapmış ve öğrencilerin bilgi güvenliği farkındalıkları, internet güvenliği, sosyal medya kullanımı, ağ güvenliği, şifre oluşturma ve sosyal medya tuzakları olmak üzere 5 alt boyutta çıktığı anlaşılmıştır. Başdinkçi (2017), sağlık kurumlarında bilgi güvenliği risk değerlendirilmesi üzerine yapmış olduğu çalışmada, katılımcılara göre en önemli risk faktörlerinin hasta bilgilerinin sızdırılması, şifrenin paylaşılması, kötü niyet, veri güvenliğinin sağlanamaması ve lisanssız yazılım kullanımı olduğu sonucuna varmıştır. Henkoğlu (2017), kişisel veri güvenliği ve bilgi güvenliği konusunda yapmış olduğu değerlendirme çalışmasında, bilgi güvenliği konusunda uygulamada yapılan yanlışlar ve bu konudaki sorumlulukların neler olduğu, teknik ve hukuki boyutu, uygulamadaki risklerin neler olduğu konularında bir çalışma yapmıştır. Yılmaz vd. (2016), öğretmenlerin dijital veri güvenliği farkındalığını ölçmek

amacıyla bir çalışma yapmışlardır. Çalışma sonucunda öğretmenlerin dijital veri güvenliğinin çok yüksek seviyede olduğu, farkındalık değerlerinin cinsiyet, kullanım sıklığı, elektronik cihaz çeşitliliği durumlarına göre değiştiği görülmüştür.

Güvenlik personelinin bilgi güvenliği farkındalık düzeylerinin tespit edilmesi amacıyla yürütülen bu çalışma mevcut durumu ortaya koyması bakımından betimleyici niteliktedir. Gerçeğin ne olduğunu bulmak ve var olan mevcut duruma anlam verilmesine dönük araştırmalar tanımlayıcı bir özelliğe sahiptir ve genellikle güncel sorunların çözümüne yönelik, pratikteki yararı gözetilerek yapılan uygulamalı araştırmalardır (Ural ve Kılıç, 2011). Diğer taraftan çalışma belirli bir yerde yapıldığı için kesitsel bir araştırma niteliği de taşımaktadır. Bu çerçevede, uygulamalı bir şekilde araştırmanın amacının gerçekleştirilmesi, Türkiye'nin jeopolitik konumu bakımından en önemli insan kaynağı bileşeni olan güvenlik personelinin bilgi güvenliği konusundaki farkındalık düzeyini ortaya koymakta olup, hangi konuda eksikliklerin olduğu belirlenerek yetkililer tarafından gerekli önlemlerin alınması açısından önemli görülmektedir.

2. MATERYAL ve METOT

Bu araştırmanın evrenini, Siirt İl merkezindeki İl Jandarma Komutanlığı ve İl Emniyet Müdürlüğünde görev yapan jandarma ve polisler oluşturmaktadır. Çalışmada zaman ve maliyet vb. nedenlerden dolayı örneklem alınma yoluna gidilmiş olup tabakalı örnekleme yöntemi ile seçilen 207 jandarma ve 197 polis olmak üzere toplam 404 personel araştırmanın örneklem grubunu oluşturmaktadır.

Çalışmada veri toplama aracı olarak anket kullanılmıştır. Söz konusu anket temel olarak 2 bölümden oluşmaktadır. Anketin birinci bölümünde emniyet personelinin sosyo-demografik ve diğer bazı bireysel özelliklerini belirlemek üzere 11 adet kapalı uçlu soruya (mesleği, cinsiyet, medeni durum, yaş, eğitim düzeyleri, kıdem, çalıştıkları birim, unvan, sahip oldukları cihazlar, internete bağlanılan cihazlar, bilgisayar ve bilgi güvenliği seviyeleri) yer verilmiş olup anketin ikinci bölümünde ise Keser ve Güldüren (2015) tarafından geliştirilen 2 boyut (saldırı ve tehditler; kişisel verileri koruma) ve 34 maddeden oluşan bilgi güvenliği farkındalığı ölçeğine yer verilmiştir. Ölçekte yer alan her bir madde 5'li likert tipi derecelendirmeye tabi tutulmuş olup 1=Hiç katılmıyorum ve 5=Tamamen katılıyorum aralığında puanlandırılmıştır.

Veriler SPSS 18.0 for Windows paket programı ile analiz edilmiş olup emniyet personelinin sosyo-demografik ve diğer bazı bireysel özellikleri frekans ve yüzde dağılımı ile sunulmuştur. Diğer taraftan ölçekteki her bir madde frekans ve yüzde dağılımının yanı sıra aritmetik ortalama ve standart sapma değerleriyle betimlenmiştir. Ayrıca katılımcıların bilgi güvenliği farkındalığının bireysel özelliklere göre karşılaştırılmasında parametrik test varsayımları (verilerin normal dağılması, varyansların homojenliği, gruplardaki birey sayısı vb.) gerçekleştiği için

iki grup için bağımsız örneklemler için t-testi, ikiden fazla grup için ise tek yönlü varyans analizi kullanılmıştır. Varyans analizi sonucunda farklılığın kaynağını ortaya koymak için Tukey testi uygulanmıştır. Bununla birlikte ölçeklerin güvenilirliği için Cronbach's Alpha değerleri hesaplanmıştır. Buna göre Cronbach's Alpha değerleri saldırı ve tehditler alt boyutu için 0,786; kişisel verileri koruma alt boyutu için 0,803 ve genel bilgi güvenliği farkındalığı ölçeği için ise 0,814 olarak hesaplanmıştır.

3. BULGULAR

Katılımcıların demografik özelliklerine ilişkin dağılımları Tablo 1'de sunulmuştur.

Tablo-1. Katılımcıların Bireysel Özelliklerine Göre Dağılımı

Değişken	**Grup**	**Sayı (f)**	**Yüzde (%)**
Meslek	Asker	207	51,4
	Polis	196	48,6
Cinsiyet	Kadın	60	14,9
	Erkek	343	85,1
Medeni Durum	Evli	284	70,5
	Bekar	119	29,5
Yaş	18-22 yaş	17	4,2
	23-27 yaş	147	36,5
	28-32 yaş	115	28,5
	33-37 yaş	51	12,7
	38-42 yaş	49	12,2
	43 yaş ve üzeri	24	6,0
Ünvan	Uzman Erbaş (onbaşı, çavuş v.b)	139	34,5
	Subay-Astsubay	68	16,9
	Polis Memuru	196	48,6
Çalışılan Birim	Asayiş	112	27,8
	Kaçakçılık ve Organize Suçlar	32	7,9
	Komando ve Özel Harekat	52	12,9
	Kriminal ve OYİ	14	3,5
	İstihbarat	42	10,4
	Terörle mücadele	40	9,9
	Diğer (Trafik, çevik kuvvet, siber suçlar v.b)	112	27,6
Çalışma Süresi	1 yıl ve daha az	45	11,2
	2-4 yıl	128	31,8
	5-7 yıl	97	24,1
	8-10 yıl	46	11,4
	11 yıl ve daha fazla	87	21,6
Toplam		**403**	**100,0**

Tablo 1'e göre, %51,4'ü asker iken %48,6'sı ise polistir. Katılımcıların %14,9'u kadın ve %85,1'i erkeklerden oluşurken, %70,5'i evli ve %29,5'i ise bekardır. Katılımcıların %4,2'si 18-22, %36,5'i 23-27, %28,5'i 28-32, %12,7'si 33-37, %12,2'si 38-43 ve %6,0'sı ise 43 yaş ve üzeri yaş grubunda yer almaktadır.

Örneklem grubunun %28,5'i lise ve altında, %26,6'sı önlisans ve %44,9'u Lisans ve üzerinde eğitime sahiptirler. Katılımcıların, %24,5'i uzman erbaşlardan (onbaşı, çavuş vb.), %16,9'u subay-astsubay ve %48,6'sı polis memurlarından oluşurken, %27,8'i asayiş, %7,9'u kaçakçılık ve organize suçlar, %12,9'u komando ve özel harekât, %3,5'i kriminal ve OYİ, %10,4'ü istihbarat, %9,9'u terörle mücadele ve %27,6'sı diğer (çevik kuvvet, siber suçlar v.b) birimlerde çalışmaktadırlar. Katılımcıların %11,2'si 1 yıl ve daha az süredir, %31,8'i 2-4 yıl, %24,1'i 5-7 yıl, %11,4'ü 8-10 yıl ve %21,6'sı ise 11 yıl ve daha uzun süredir meslekte çalıştıklarını belirtmişlerdir (Tablo 1).

Bilgi güvenliği farkındalık düzeyi ölçeğinin "saldırı ve tehditler" alt boyutuna ilişkin betimsel istatistikler Tablo 2'de sunulmuştur.

Tablo-2. Bilgi Güvenliği Farkındalık Düzeyi Ölçeğinin "Saldırı ve Tehditler" Alt Boyutuna İlişkin Betimsel İstatistikler

Maddeler		Katılım Düzeyi					$\overline{X}$ ±SS
		Hiç	Az	Orta	Çok	Tam	
Bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim.	f	122	96	102	44	39	2,46
	%	30,3	23,8	25,3	10,9	9,7	±1,29
Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum.	f	95	112	104	46	46	2,59
	%	23,6	27,8	25,8	11,4	11,4	±1,28
Aldatmaca (hoax) nedir biliyorum.	f	149	93	87	43	31	2,29
	%	37,0	23,1	21,6	10,7	7,7	±1,27
Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.	f	126	116	80	49	32	2,37
	%	31,3	28,8	19,9	12,2	7,9	±1,26
Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.	f	134	106	84	45	34	2,35
	%	33,3	26,3	20,8	11,2	8,4	±1,28
Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum.	f	148	84	78	56	37	2,38
	%	36,7	20,8	19,4	13,9	9,2	±1,34
Kimlik hırsızlığı (identity theft) nedir biliyorum.	f	134	93	92	46	38	2,41
	%	33,3	23,1	22,8	11,4	9,4	±1,31

Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.	f	138	90	94	47	34	2,38
	%	34,2	22,3	23,3	11,7	8,4	±1,29
Sahte virüs koruma yazılımının ne olduğunu biliyorum.	f	119	105	85	54	40	2,48
	%	29,5	26,1	21,1	13,4	9,9	±1,31
Hizmet aksatrma (Denial of Service - DoS) saldırısı nedir biliyorum.	f	194	77	72	37	23	2,05
	%	48,1	19,1	17,9	9,2	5,7	±1,24
Kimlik avı (phishing) saldırısı nedir biliyorum.	f	155	103	86	37	22	2,18
	%	38,5	25,6	21,3	9,2	5,5	±1,20
Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.	f	175	86	78	41	23	2,13
	%	43,4	21,3	19,4	10,2	5,7	±1,24
Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.	f	170	84	83	41	25	2,17
	%	42,2	20,8	20,6	10,2	6,2	±1,25
Siber zorbalık (cyberbullying) nedir biliyorum.	f	148	95	80	52	28	2,30
	%	36,7	23,6	19,9	12,9	6,9	±1,27
Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.	f	157	86	81	48	31	2,28
	%	39,0	21,3	20,1	11,9	7,7	±1,30
Siber zorbalığa karşı çocuklarımı nasıl koruyacağımı biliyorum.	f	149	87	75	58	34	2,36
	%	37,0	21,6	18,6	14,4	8,4	±1,33

Tablo 2 incelendiğinde, "kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum" maddesine katılımcıların %53,6'sı az ve orta seçenekleri ile ($\bar{x}$=2,59), "sahte virüs koruma yazılımının ne olduğunu biliyorum" maddesine katılımcıların %47,2'sinin az ve orta seçenekleri ile ($\bar{x}$=2,48) ve "bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim" maddesine katılımcıların %49,1'inin az ve orta ($\bar{x}$=2,46) seçenekleri ile yarı olumlu görüş belirtmişlerdir. Ayrıca katılımcıların %67,2'si "hizmet aksatma (Denial of Service - DoS) saldırısı nedir biliyorum" maddesine hiç ve az seçenekleri, ($\bar{x}$=2,05), "sosyal mühendislik (social engineering) saldırısı nedir biliyorum" maddesine katılımcıların %64,7'si ($\bar{x}$=2,13) hiç ve az seçenekleri ve "sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum" maddesine katılımcıların %63,0'ı hiç ve az ($\bar{x}$=2,17) seçenekleri ile olumsuz görüş bildirmişlerdir.

Katılımcıların bilgi güvenliği farkındalık düzeyi ölçeğinin "kişisel verileri koruma" alt boyutuna ilişkin betimsel istatistikler Tablo 3'te sunulmuştur.

Tablo-3. Bilgi Güvenliği Farkındalık Düzeyi Ölçeğinin "Kişisel Verileri Koruma" Alt Boyutuna İlişkin Betimsel İstatistikler

Maddeler		**Katılım Düzeyi**					$\overline{X}$
		Hiç	**Az**	**Orta**	**Çok**	**Tam**	**±SS**
Bilgi güvenliğinin ne anlama geldiğini biliyorum.	f	85	93	96	71	58	2,81
	%	21,1	23,1	23,8	17,6	14,4	±1,34
Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.	f	90	93	88	77	55	2,79
	%	22,3	23,1	21,8	19,1	13,6	±1,35
Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.	f	98	96	91	66	52	2,70
	%	24,3	23,8	22,6	16,4	12,9	±1,34
Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum.	f	103	99	83	64	54	2,67
	%	25,6	24,6	20,6	15,9	13,4	±1,36
Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım.	f	106	95	89	52	61	2,67
	%	26,3	23,6	22,1	12,9	15,1	±1,38
Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.	f	93	84	87	63	76	2,86
	%	23,1	20,8	21,6	15,6	18,9	±1,42
Dijital imza (digital signature) nedir biliyorum.	f	95	69	94	76	69	2,89
	%	23,6	17,1	23,3	18,9	17,1	±1,41
Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.	f	81	69	99	66	88	3,03
	%	20,1	17,1	24,6	16,4	21,8	±1,42
E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.	f	102	82	99	59	61	2,74
	%	25,3	20,3	24,6	14,6	15,1	±1,38
İstenmeyen elektronik posta (spam) nedir biliyorum.	f	84	77	104	52	86	2,95
	%	20,8	19,1	25,8	12,9	21,3	±1,42
İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.	f	111	88	78	51	75	2,73
	%	27,5	21,8	19,4	12,7	18,6	±1,46
Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı biliyorum.	f	97	85	101	52	68	2,77
	%	24,1	21,1	25,1	12,9	16,9	±1,39

USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.	f	78	83	90	63	89	3,00 ±1,42
	%	19,4	20,6	22,3	15,6	22,1	
Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.	f	85	78	103	57	80	2,92 ±1,40
	%	21,1	19,4	25,6	14	19,9	
Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.	f	81	92	93	60	77	2,90 ±1,39
	%	20,1	22,8	23,1	14,9	19,1	
Kişisel mahremiyet nedir biliyorum.	f	72	65	89	73	104	3,18 ±1,44
	%	17,9	16,1	22,1	18,1	25,8	
Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.	f	71	91	91	64	86	3,01 ±1,40
	%	17,6	22,6	22,6	15,9	21,3	
Mavidiş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.	f	95	73	78	69	88	2,96 ±1,47
	%	23,6	18,1	19,4	17,1	21,8	

Tablo 3'e göre, "Kişisel mahremiyet nedir biliyorum." ($\bar{x}$=3,18) maddesine katılımcıların %43,9'u çok ile tam seçenekleri, "şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum" ($\bar{x}$=3,03) maddesine katılımcıların %38,2'si çok ile tam secenekleri ve "çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum" ($\bar{x}$=3,01) maddesine katılımcıların %37,2'si çok ile tam seçenekleri ile olumlu görüş bildirmişlerdir. Bunun yanı sıra katılımcıların, %50,2'si "bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum" ($\bar{x}$=2,67) maddesine hiç ve az, %49,9'u "bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım" ($\bar{x}$=2,67) maddesine hiç ve az ve %48,1'i "kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum" ($\bar{x}$=2,70) maddesine hiç ve az seçenekleri ile olumsuz görüş bildirmişlerdir.

Katılımcıların bilgi güvenliği farkındalık düzeyleri bireysel özelliklerine göre karşılaştırılmış olup, farklılık bulunan değişkenlere ilişkin varyans analizi sonuçları Tablo 4'te sunulmuştur.

Tablo-4. Katılımcıların Bilgi Güvenliği Farkındalığının Bazı Bireysel Özelliklere Göre Karşılaştırması

Değişken	Grup	$\overline{X}$	SS	F	p
Yaş	18-22 yaş	2,49[ab]	0,76		
	23-27 yaş	2,37[b]	1,01		
	28-32 yaş	2,88[a]	1,04	3,218	0,007*
	33-37 yaş	2,68[ab]	0,97		
	38-42 yaş	2,69[ab]	1,25		
	43 yaş ve üzeri	2,56[ab]	1,15		
Eğitim Düzeyi	Lise ve altı	2,27[c]	1,07		
	Ön lisans	2,58[b]	0,96	5,588	0,000*
	Lisans	2,84[a]	1,06		
Meslek	Uzman Erbaş	2,36[b]	1,09		
	Subay-Astsubay	2,90[a]	1,08	7,413	0,001*
	Polis Memuru	2,69[ab]	1,00		
Birim	Asayiş	2,31[c]	1,09		
	Kaçakçılık ve Organize Suçlar	2,41[c]	0,83		
	Komando ve Özel Harekat	2,63[b]	0,89		
	Kriminal ve OYİ	3,61[a]	1,25	4,886	0,000*
	İstihbarat	2,94[b]	1,02		
	Tem	2,90[b]	0,99		
	Diğer	2,45[c]	1,15		

*$p<0,05$; *a,b,c:aynı sütunda farklı harfleri içeren gruplar arasındaki farklar önemlidir.*

Tablo 4'teki bulgulara göre personelin bilgi güvenliği farkındalık düzeyleri yaşa, eğitim düzeyine, mesleğe ev çalışılan birime göre anlamlı farklılıklar göstermiştir ($p<0,05$). Ortalama değerleri incelendiğinde, bilgi güvenliği farkındalığı en yüksek olan gruplar, 28-32 yaş arası personel, lisans mezunu personel, subay-astsubay, kriminal ve OYİ (Olay Yeri İnceleme) birimlerinde çalışanlardan oluşmaktadır.

SONUÇ

Kişisel ve özelliklede kurumsal anlamda sahip olunan bilgideki yoğun artış ile bilgiye başka yer, mekân ve platformlardan ulaşılabilme gereksinimi bilginin dijital ortamlara aktarılmasına yol açmıştır. Teknolojik gelişmelerin ışığında bilginin depolanması, iletimi ve bilgiye ulaşılması hem daha kolay hem de daha hızlı olmuştur. Bu durum kurumun faaliyet gösterdiği her bölgede aynı bilgi seviyesi ile hizmet vermesini ve kurumsal hafızanın oluşmasını sağlamıştır. Dijital ortamlara aktarılan bu bilginin korunması kişisel ve kurumsal anlamda hayati önem arz eden bir konu haline gelmiştir (Çetin, 2014).

Teknolojik gelişmelere paralel olarak bilgi güvenliğini sağlayan teknik detaylar da gelişmiş ve her geçen gün yapılan yeni güncellemelerle elektronik ortamlardaki açıklıklar giderilmektedir. Bu durum kötü niyetli şahısların bilginin kontrolünü ele

geçirebilmek için kurumlardaki bu bilgi teknolojilerini kullanan insan unsuru üzerinde yoğunlaşmasına yol açmıştır. Bu nedenle bir kurumdaki güvenlik seviyesinin en zayıf halkası kuşkusuz insan unsurudur. Kritik kamu kurumlarında çalışan ve ülke menfaatlerinin tehlikeye atabilecek bilgiye ulaşan personel bilinçli veya bilinçsiz yaptığı her türlü ihlal ülke güvenliği açısından tehlikeli boyutlara varabilmektedir. Bilinçli yapılan bilgi güvenliği ihlallerine karşı personel alım sürecindeki arşiv ve güvenlik araştırmaları yeterli olabilecekken personelin bilinç dışı yaptığı ihlaller ancak kişilerin bilinçlendirilmesi ve bilgi güvenliği altyapısının oluşturulabilmesi ile mümkün olabilecektir (Tekerek, 2008; Yılmaz vd., 2016; Erdoğmuş, 2017; Keser ve Güldüren, 2015).

Yukarıdaki bilgiler çerçevesinde, emniyet ve asayiş ile kamu düzenini korumakla görevli olan, toplum huzuru ve ülke menfaatleri çerçevesinde suç önleyici çalışma yürüten ve bu çalışmaları yürütürken birçok gizli bilgiyi de bünyesinde barındıran güvenlik (polis, jandarma) personelinin bilgi güvenliği farkındalık düzeylerinin tespit edilmesi amacıyla yapılan bu çalışmaya 207 jandarma ve 197 polis olmak üzere toplam 404 personel katılmıştır. Araştırma sonucunda, bilgi güvenliği farkındalık düzeyi ölçeğinin "saldırı ve tehditler" alt boyutuna ilişkin genel ortalama 2,32 ve "kişisel verileri koruma" alt boyutuna ilişkin genel ortalama ise 2,87 olarak hesaplanmıştır. Bu değerler Likert tipi ölçekte orta düzeyi gösteren 3 puanın altındadır ve emniyet personelinin (polis, jandarma) bilgi güvenliği farkındalık düzeylerinin düşük olduğunu göstermektedir. Özellikle emniyet personelinin "saldırı ve tehditler" alt boyutundaki bilgi güvenliği farkındalık düzeylerinin düşük olması dikkat çeken bir sonuç olmuştur. Bunu nedeni, saldırı ve tehdit konusunun diğer konulara oranla daha spesifik ve ilgi gerektiren bir konu olması olabileceği, ancak kurumsal bilgisayar kullanan personelin asgari düzeyde bu konularla içli dışlı olması kurumun siber saldırılara ve kurumun sahip olduğu bilginin yetkisiz kişilerin eline geçmesine karşı almış olacağı ilk önlem olabilecektir. Bilgi güvenliği farkındalık düzeyinin genel olarak düşük olmasının sebebi ise, kurum içi eğitimlerin alım süreci, oryantasyon eğitimi, hizmet içi eğitim süreçlerinde yetersiz seviyede olması gösterilebilir. Kurum içerisinde çalışan tüm personelin bilgi güvenliği konusunda asgari seviyeye gelebilmesi için eğitim faktörü öne çıkan ilk seçenektir.

Bilgi güvenliği farkındalık ölçeğinin "saldırı ve tehditler" alt boyutu incelendiğinde; güvenlik personelinin, kötü niyetli yazılımlara karşı alınması gereken güvenlik tedbirleri, sahte virüs koruma yazılımının ne olduğu, bilgisayara kötü niyetli kod bulaşıp bulaşmadığının anlaşılması konularında diğer ölçek maddelerine oranla daha iyi seviyede olması ile birlikte, hizmet aksatma saldırıları, sosyal mühendislik saldırıları ve sosyal mühendislik saldırılarına uğramamak için nasıl hareket etmesi konularında diğer ölçek maddelerine oranla daha düşük seviyede olduğu görülmüştür. Yine Bilgi Güvenliği Farkındalık Ölçeğinin "kişisel verileri koruma" alt boyutuna ilişkin veriler incelendiğinde; kişisel mahremiyetin

ne olduğu, şüpheli veya bilinmeyen kaynaklardan gelen e-postaları açmanın taşıdığı risk, çevrim içi güvenli alışveriş yapmak için alınması gereken güvenlik tedbirleri alt boyutlarında güvenlik personelinin diğer ölçek alt boyutlarına oranla daha iyi seviyede oldukları ancak, virüs koruma yazılımını nasıl kullanması gerektiği, virüs koruma yazılımının gerçek zamanlı koruma özelliğinin kullanılması, bilgi sistemlerindeki tanımlanmış olan kuralları nasıl uygulayacağı konularında diğer ölçek boyutlarına oranla daha düşük seviyede oldukları görülmüştür.

Araştırma sonucunda güvenlik personelinin bilgi güvenliği farkındalık düzeyinin yaşa, eğitime, çalışılan birim ve mesleğe göre anlamlı farklılıklar gösterdiği tespit edilmiştir. Buna göre 28-32 yaş arası, lisans mezunu, subay-astsubay, kriminal ve OYİ (Olay Yeri İnceleme) birimlerinde çalışanların bilgi güvenliği farkındalığının diğer gruplara göre daha yüksek olduğu saptanmıştır. Bu durumun kriminal, olay yeri ve siber suçlar bölümlerinde çalışan personelin bilgisayar konusunda daha çok bilgiye sahip olmasından, daha özel ve uzmanlık gerektiren işler ile uğraşmasından kaynaklandığı değerlendirilebilir.

Yılmaz vd. (2016)'nin öğretmenlerin dijital veri güvenliğini ölçmek amacıyla yapmış oldukları çalışmada farkındalık düzeyinin yaş ve kullanım sıklığı ile ilişkili olduğu sonucu ile Karadağ ve Abuhanoğlu (2015)'nun Gülhane Askeri Tıp akademisi çalışanlarının bilgi güvenliği farkındalık seviyesini belirlemek üzere yapmış oldukları çalışmada farkındalık düzeyinin yaş ve unvan faktörleri ile ilişkili olduğu belirtilmiştir. Ayrıca Akgün ve Topal (2005)'ın eğitim fakültelerinde eğitim gören öğrencilerin bilgi güvenliği seviyelerini araştırmak üzere yapmış oldukları çalışmada bilgi güvenliği konusunda eğitim alan ve almayanlar arasında ciddi bir fark olduğu sonucu ile bu çalışmadaki kriminal, olay yeri inceleme birimlerinin siber bölümlerinde çalışan personelin bilgisayar konusunda aldığı eğitim göz önüne alındığında benzer sonuca ulaşmıştır.

Yukarıdaki sonuçlar çerçevesinde konu ile ilgili farklı çalışmaların farklı illerde farklı örneklemlerle yapılması bilgi güvenliği farkındalık düzeyinin mevcut durumunu betimleyecek, literatüre önemli katkılar sunacak ve ilgili birimlerin önlem alması konusunda yöneticilere önemli veri kaynağı oluşturacaktır. Bu anlamda çalışmanın sonuçlarından hareketle; güvenlik personelinin (polis, jandarma) mesleğe başlamadan önceki eğitim ve oryantasyon eğitimi aşamalarında temel bilgisayar eğitiminin yanında bilgi güvenliği ve farkındalık konularında gerekli ders ve sınavlar ile farkındalığın oluşturulması personelin meslek hayatı boyunca bu konuda belli bir seviyeye gelmesi açısından son derece önemli olduğu değerlendirilmektedir. Ayrıca bilgi güvenliği üzerinde uzmanlaşmış kişi ve kuruluşlar yardımı ile meslek içi eğitim ve seminerler düzenlenerek konunun pekiştirilmesi ve yeni teknolojik gelişmelerin takip edilmesi açısından gerekli olduğu değerlendirilmektedir.

KAYNAKÇA

Akgün, Ö. E. ve Topal, M. (2015). Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği. 8. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu bildiriler kitabı içinde (ss. 98-121), Sakarya,

Aydın, M. (2004). Bilgi sosyolojisi. İstanbul: Açılım Kitap.

Başdinkçi, N. (2017). Sağlık Kurumlarında Bilgi Güvenliği Risk Değerlendirilmesi ve Kullanıcıların Bilgi Güvenliği Farkındalık Düzeyinin Ölçülmesi. (Yüksek Lisans Tezi). Çukurova Üniversitesi, Adana.

Bolat, Y. İ., Aydemir, M., ve Karaman, S. (2017). Uzaktan Eğitim Öğrencilerinin Öğretimsel Etkinliklerde Mobil İnternet Kullanımlarının Teknoloji Kabul Modeline Göre İncelenmesi. Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi, 37(1), 63-91.

Canbek, G., ve Sağıroğlu, Ş. (2006). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. Gazi Mühendislik ve Mimarlık dergisi. 22(1), 121-136

Çek, E. (2017). Kurumsal Bilgi Güvenliği ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi. (Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi, İstanbul.

Çetin, H. (2014). Kişisel Veri Güvenliği Ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesİ. Akdeniz Üniversitesi İktisadi ve İdari Birimler Fakültesi Dergisi, (29), 86-105.

Davenport, T., & Prusak, L. (2001). İş Dünyasında Bilgi Yönetimi, İstanbul: Rota Yayınları, Çevirmen :Günhan GÜNAY.

Demirtaş, H. (2013). Bilgi Güvenliği Yönetiminin Gerekleri Ve Başarı Dayanakları: Bir Uygulama Örneği. (Yüksek Lisans Tezi). Sakarya Üniversitesi, Sakarya.

Eminağaoğlu, M., ve Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye' de Bilgi Güvenliği Sorunları ve Çözüm Önerileri . Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi , 11(4), 01-15.

Erdoğmuş, A. (2017). Üniversite Öğrencilerinin Bilgi Güvenliği Kazanimlarinin, Farkindaliklari Üzerindeki Etkilerinin Analizi: Afyon Kocatepe Üniversitesi Örneği. (Yüksek Lisans Tezi). Afyon Kocatepe Üniversitesi, Afyon.

Ertuğrul, İ., ve Keskin, N. (2012). İnternet'İn Türkçenin Kullanımında Ve Toplum-Birey Yapısının Değişimindeki Rolü. Doğu Akdeniz Üniversitesi, Bilgisayar ve Teknoloji Yüksek Okulu, Mesleki Eğitim Sempozyumu, 3(2), 80-88

Güçlü, N., ve Sotirofski, K. (2006). Bilgi Yönetimi. Türk Eğitim Bilimleri Dergisi, 4(4), 351-371.

Gülmüş, M. (2010). Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği. (Yüksek Lisans Tezi). Yıldız Teknik Üniversitesi, İstanbul.

Henkoğlu, T. (2017). Kişisel Verilerimiz Ne Kadar Güvende: Bilgi Güvenliği Kapsamında Bir Değerlendirme. Arşiv Dünyası Dergisi, 17(18), 46-56.

Irzık G. (2002). Bilgi Toplumu mu, Enformasyon Toplumu mu, Analitik ve Eleştirel Bir Yaklaşım. Türkiye Bilimler akademisi Yayınları, 53-62.

Karaaslan, E. (2013). Siber Güvenlik Deneyleri için Ağ Benzetici ve Ağ Sınama Ortamlarının Kullanımına Dair Ön İnceleme . Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 1-7.

Karadağ, M., ve Abuhanoğlu, H. (2015). Sosyo-Kültürel Özelliklerin Bilgi Güvenliği Farkındalığı Üzerine Etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesinde Bir Çalışma. International Journal of Social Science, Doi : 10.9761/ JASSS288436, 36, 379-386.

Keser, H., ve Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği Geliştirme Çalışması. Kastamonu Üniversitesi Eğitim Dergisi, 23(3), 1167-1184

Mart, İ. (2012). Bilişim Kültüründe Bilgi Güvenliği Farkındalığı. (Yayımlanmamış Yüksek Lisans Tezi). Kahramanmaraş Sütçü İmam Üniversitesi, Kahramanmaraş.

Mengüşoğlu, T. (1988). İnsan Felsefesi. İstanbul: Remzi Yayınevi.

Odabaş, H. (2003). Kurumsal Bilgi Yönetimi. Türk Kütüphaneciliği, 17(4), 357-368.

Sayarı, N. (2009). Bilgi Güvenliği ve Yönetimi. Türkiye Bilişim Derneği Ankara Şubesi Eğitim Etkinliği. Ankara.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., ve Borandağ, E. (2009). Kurmlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri. 11. Akademik Bilişim Konferansı bildiriler kitabı içinde (ss. 597-602) Harran Üniversitesi, Şanlıurfa.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. KSÜ Fen ve Mühendislik Fakültesi Dergisi 11(1), 132-137

Türk, M. (2003). Küreselleşme Sürecinde İşletmelerde Bilgi Yönetimi. İstanbul: Türkmen Kitabevi.

Ural, A., Kılıç, İ. (2011). Bilimsel Araştırma Süreci ve SPSS ile Veri Analizi. Ankara: Detay Yayıncılık.

Vural, Y. (2007). Kurumsal Bilgi Güvenliği ve Sızma Testleri. (Yüksek Lisans Tezi), Gazi Üniversitesi, Ankara.

Yeniçeri, Ö., ve İnce, M. (2005). Bilgi Yönetim Stratejileri ve Girişimcilik. İstanbul: IQ Kültür Sanat Yayıncılık.

Yılmaz, E., Şahin, Y. L., ve Akbulut, Y. (2016). Öğretmenlerin Dijital Veri Güvenliği Farkındalığı. Sakarya Üniversitesi Eğitim Bilimleri Dergisi, 6(2), 26-45.

Yılmaz, F. G., ve Ezin, Ç. (2017). Ebeveynlerin Bilgi Güvenliği Farkındalıklarının İncelenmesi. Eğitim Teknolojisi Kuram ve Uygulama Dergisi, 7(2), 41-57.

Yılmaz, M. (2009). Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi. Ankara Üniversitesi Dil ve Tarih Coğrafya Fakültesi Dergisi, 49(1), 95-118.