TÜRKİYE SOSYAL ARAŞTIRMALAR DERGİSİ
YIL: 25 SAYI 3 – Aralık 2021
Makalenin Geliş Tarihi: 23.10.2020 Makalenin Kabul Tarihi: 13.10.2021 Sayfa: 649-666

KAMU KURUM VE KURULUŞLARINDA BİLGİ GÜVENLİĞİ FARKINDALIĞI[*]

Ayşe ÖZDEMİR[**]
Çelebi ULUYOL[***]

ÖZ

Bu çalışmanın amacı kamu çalışanlarının bilgi güvenliği farkındalıklarını ortaya koymaktır. Araştırma nicel araştırma yöntemlerinden betimsel tarama modeli kullanılarak yürütülmüştür. Araştırma kamu kurum ve kuruluşlarında çalışan 302 erkek ve 199 kadın olmak üzere 501 kişi ile gerçekleştirilmiştir. Veri toplama aracı olarak Bilgi Güvenliği Farkındalık Ölçeği kullanılmıştır. Ölçeğin Cronbach alfa güvenilirlik katsayısı .97' dir. Ölçek otuz dört soru ve iki alt boyuttan oluşmaktadır. Ölçekte ilk alt boyut saldırı ve tehditler, ikinci alt boyut ise kişisel verilerin korunmasıdır. Çalışanlardan cinsiyet, yaş aralığı, eğitim durumu ve çalıştığı birim olmak üzere çeşitli demografik ve ölçek sorularını cevaplamaları istenmiştir. Çalışma sonunda kamu çalışanlarının ölçek genelinden aldıkları ortalama puana göre orta seviyede bilgi güvenliği farkındalığına sahip oldukları görülmüştür. Erkek ve kadın katılımcıların benzer seviyede bilgi güvenliği farkındalığına sahip oldukları, 40 yaş altı katılımcılar ile teknik eğitim almış olan bilgi teknolojileri çalışanlarının ise bilgi güvenliği farkındalık seviyelerinin yüksek olduğu görülmüştür. Çalışmada üniversite düzeyinde eğitim seviyesine sahip olan katılımcıların lise ve altı eğitim seviyesine sahip olan katılımcılara göre daha yüksek bilgi güvenliği farkındalığına sahip oldukları görülmüştür. Bilgi güvenliğinin sürekli yenilenen bir süreç olduğu noktasından hareketle, çalışanlara yönelik verilen eğitimlerin yenilikleri barındıracak biçimde güncellenmesi, çalışanların güvenlik farkındalıklarının sağlanabilmesi ve sürdürülebilirliği açısından önem arz etmektedir.

Anahtar Kelimeler: Bilgi güvenliği, farkındalık, kamu çalışanı

INFORMATION SECURITY AWARENESS IN PUBLIC ORGANIZATIONS

ABSTRACT

The study aims to reveal the information security awareness of public employees. The research is a descriptive survey model. The research was conducted with 501 people, 302 males and 199 females, working in public organizations. Information Security Awareness Scale was used as data collection tool. The Cronbach's alpha reliability coefficient of the scale was .97. In this study, the Cronbach alpha reliability coefficient was once again calculated as .97 for the whole scale. The scale consists of thirty-four questions and two sub-dimensions. The first sub-dimension of the scale is attacks and threats, and the second sub-dimension is the protection of personal data. The employees were asked to answer the questions of the scale, including gender, age range, education, and unit where they worked. At the end of the study, it was seen that public employees had a moderate level of information security awareness based on the average score they received from the overall scale. Among the participants, male and female participants had a similar level of information security awareness and the information security awareness levels of Information Technology employees who were under the age of 40 with technical training were high. Also, it was seen that the participants who have university-level education have higher information security awareness than those who have higher education level or lower. Starting from the point that information security is a process that is renewed, updating the training provided for employees to accommodate innovations is crucial in terms of ensuring safety awareness and sustainability of employees.

Keywords: Information security, awareness, public employee

GİRİŞ

Bilgi ve iletişim teknolojilerindeki gelişmeler günlük hayatımızı kolaylaştırmakta ve sağladığı imkânlarla kendini vazgeçilmez hale getirmektedir. Bilgi insanlığın en başından beri kıymetli kabul ettiği bir varlık olarak hangi ortamda saklanırsa saklansın kullanıcısı ve sahibi tarafından korunmaya muhtaç olmuştur. Bilginin korunma gereği onun güvenliğini sağlama yöntemlerini ve bilgi güvenliği kavramını hayatımıza katmıştır. Bilgi güvenliğinin temel unsurları olan gizlilik, bütünlük ve erişilebilirlik sağlanarak bilginin korunabileceğine dair bilgi güvenliği modelleri oluşturulmuştur

[*] Bu makale Ayşe ÖZDEMİR'in yüksek lisans tez çalışmasından üretilmiştir.

[**] Yüksek lisans, Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim ABD. ayseozdemir807@gmail.com, ORCID: https://orcid.org/0000-0002-4812-3072

[***] Doç. Dr., Gazi Üniversitesi Gazi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi, celebi@gazi.edu.tr, ORCID: https://orcid.org/0000-0001-9774-0547

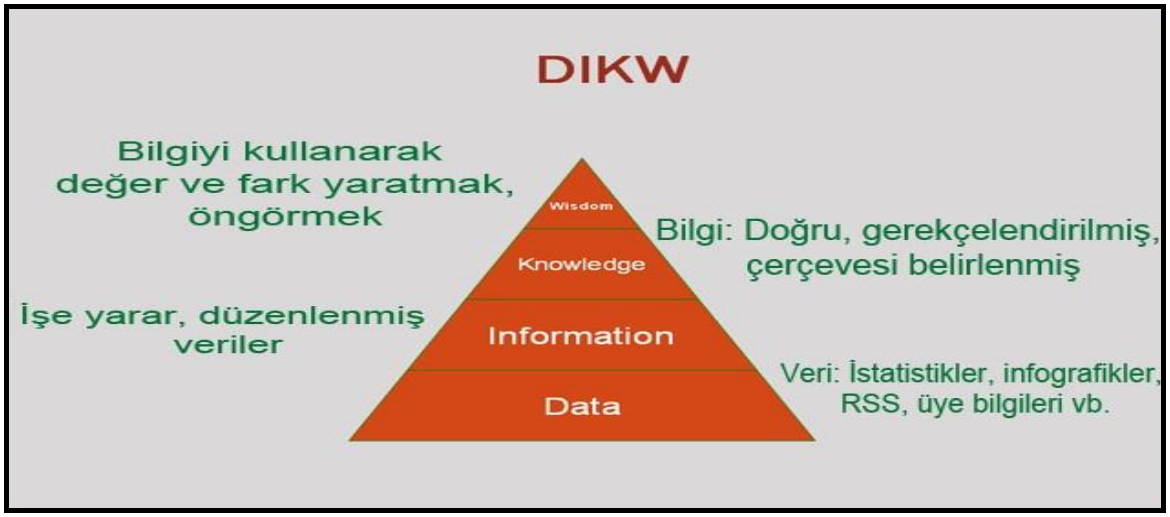
(Boyacı, Benzer ve Ciylan, 2016).

Bilgi güvenliği politikaları her ne kadar tedbirli ve sıkı oluşturulsa dahi sistem içindeki en zayıf halkalardan birisi insandır. İnsanın göz ardı edilmesi ciddi risklerin ortaya çıkmasına neden olabilir. İnsandan kaynaklanan açıklardan dolayı güvenlikle ilgili tehlikenin boyutu da değişmektedir. İnternetin hayatımızda yaygınlaşmasıyla birlikte bu riskler ve tehditler kullanılan bilgi sistemiyle aynı ortamda bulunmadan uzaktan yapılan saldırılar haline gelmiştir. Son yıllarda siber saldırıların boyutu değişmiş, bireysel saldırılar yanında çok ciddi ülkeler arası saldırılar yaşanmaya başlamıştır. Bu saldırılardan en çok etkilenen beş sektör arasında kamu kurum ve kuruluşları da bulunmaktadır (Bıçakçı, Ergün ve Çelikpala, 2015). Kamu kurumları aynı zamanda kritik sektörler arasında da yer aldığı için bu kurumda görev yapan tüm çalışanların iş süreçlerinde daha dikkatli çalışması, yapacakları hataların nelere neden olabileceğinin bilincinde ve farkında olarak sorumluluklarını yerine getirmesi, hem kurumsal bilgi güvenliği hem de ulusal bilgi güvenliği açısından önem arz etmektedir. İnternetin sunduğu olanaklar sebebiyle pek çok kamu kurum ve kuruluşunun çoğu hizmeti elektronik ortamlar üzerinden kullanıcıya sunması kullanıcı ve çalışanların bilgi güvenliği farkındalığının önemini daha da artırmaktadır.

BİLGİ NEDİR?

Bilim sayesinde gelişen ve teknolojinin baş döndürücü şekilde ilerlemesiyle birlikte pek çok kavram yeni boyutlar kazanmıştır. Bilgi kök itibariyle bilmek kelimesinden geldiğini bildiğimizden bilmek arzusu ile yanan insanoğlunun bilgiye ne kadar önem verdiği ilk insandan beri bilinmektedir. İlk insandan beri tüm din, felsefe ve ilim alanlarında bilgi çok kıymetli bir varlık olmuştur. Günümüzde bilgi kelimesini sıkça kullanılmasına rağmen kesin bir tanım yapmak mümkün değildir. Sparrow (2008)' a göre bilgi günlük yaşamda öğreti, sezgi, his ve yargı gibi kavramlarla iç içe geçmiştir. İngilizcede kullanılan data, information, knowledge gibi kavramlarının çoğunun karşılığının dilimizde bilgi olarak karşılık bulması da kafa karışıklığını artırmaktadır. Bu terimlerin karşılığını bilgi piramidi ile anlatmak aradaki farkın anlaşılmasına yardımcı olacaktır.

Şekil 1'de verilen bilgi piramidine bakıldığında bilgiye ulaşmanın kolay bir iş olmadığı anlaşılır. En alttan yukarıya doğru daha çok çaba ve çalışma gerektirmektedir. Her bir aşama genellikle atlanmadan geçilir ve yukarı doğru çıkıldıkça elde bulunan şeyin miktarı azalırken değeri inanılmaz derecede artar. Bütün bu zorluklardan sonra aşağı basamakta verinin paylaşımı kolay iken yukarı basamaklarda bilginin paylaşımı zorlaşır.



Şekil 1. Bilgi piramidi (DIKW Hiyerarşisi ve Dijital Devrim, 2011)

Veri (Data): İşlenmemiş ve ham halde bulunan parçalara verilen isimdir (Bennet ve Gabriel, 1999).

Enformasyon (Information): Bir amaca yönelik olarak verinin düzenlenmesine verilen isimdir (Davenport ve Prusak, 2001).

Bilgi, Malumat (Knowledge): Enformasyon ile tecrübenin birleştirilerek anlamlı bir yapı içerecek şekilde sunulmasına verilen isimdir (Brakensiek, 2002). Başka bir deyişle, enformasyon birbiriyle ilişkisi olan anlamlandırılmış veri, bilgi ise değeri olan enformasyondur (Erol, Şahin, Yılmaz, Haseski, 2015; Şimşek, Okul, Hafçı ve Barış, 2018). Verilerin bir araya getirilip anlamlandırılmasıyla enformasyon oluşturulsa malumat bu bilgilerin toplamından çok daha değerli bir varlıktır.

Hikmet (Wisdom) : Bilgelik diye adlandırılan hikmet ise mevcut ve sahip olunan malumatın nasıl kullanılacağı, nasıl karar verileceği, nasıl değerlendirileceği yönünde bir keşif ve buluş aşamasıdır. Hikmet, güvenilir bir sonuca varmak ve doğru karar vermek için bilginin nerede, nasıl, ne şekilde kullanılacağını kavramak olarak tanımlanmaktadır (Canbek ve Sağıroğlu, 2006).

Bilginin çok kıymetli ve önemli olması bilgiye sahiplik konusunda bazı düzenlemeleri ve şartları da beraberinde getirmektedir. Bilgi sadece kişiler için değil, kurum ve ülkeler için de elde edilmesi ve korunması zor bir metadır. Bu metanın korunması hayati bir önem arz ederken onu elde etmede zorluklar yaşayan özel ya da tüzel kişilerin haklarını korumayı hem de bilginin kullanımındaki karmaşa, yozlaşma ve kötüye kullanılmasının da önüne geçecektir. Bunun için telif hakkı, patent gibi önlemler alınmıştır. Ancak bilginin korunması elektronik ortamda çok daha zordur. Bu sebeple bilgi güvenliği, dünya gündeminde ilk sıralarda yer almakta ve bu konuda yapılan çalışmalar giderek artmaktadır.

BİLGİ GÜVENLİĞİ

Bilgi güvenliği, bilgiye erişim yetkisi olan kişilerce güvenilir ve her an erişilebilir ortamda tutulması ve bilgiyi gönderen ve alan taraflar arasında bozulmadan güvenli bir şekilde iletilmesi olarak tanımlanmıştır (Ünver, Canbay ve Mirzaoğlu, 2011). Ancak bilişim teknolojilerinin gelişmesiyle birlikte dijital veri güvenliği kavramı ortaya çıkmıştır. Canbek ve Sağıroğlu (2006)'na göre dijital veri güvenliği, sayısal ortamlarda verilerin veya bilgilerin saklanması ve iletilmesi işleminde iletilen şeyin bütünlüğü bozulmadan, yetkisiz erişimlerden korunması güvenilir bir ortam oluşturulmasına dair yapılan işlemlerin tümüdür. Başka bir tanımda ise "*bilgi varlıklarının güvenliğini tehdit eden her türlü tehlikeden korunması için bilgi güvenliğini sağlayacak doğru teknolojinin, doğru zamanda doğru yerde doğru şekilde kullanılması"* olarak tanımlanır (Güngör, 2015).

Bilgi güvenliği bilginin koruyucusu ve sahibine göre çeşitli şekillerde gruplanabilmektedir (Güngör, 2015). Bu gruplar;

- Kişisel Veri Güvenliği,
- Kurumsal Bilgi Güvenliği,
- Ulusal Siber Güvenlik olarak adlandırılmaktadır.

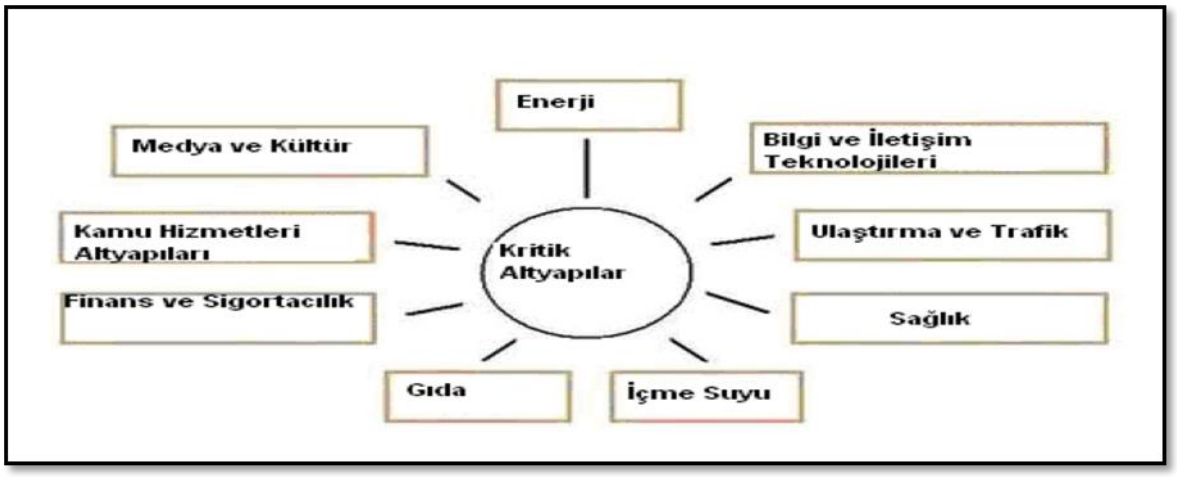
İsimler üzerinden anlaşılacağı gibi bilginin sahibi ve kıymeti büyüdükçe isimler de değişiklik göstermektedir. Kişisel veri, Kişisel Verileri Koruma Kanunu'na göre (KVKK, 2018), belirli bir kimliğe sahip veya kimliği tespit edilebilir gerçek kişiye ait her türlü veri olarak tanımlanmıştır. Bu tanım çerçevesinde kişinin kimlik bilgileri, banka bilgileri, bilgisayarının ip adresi, elektronik posta adresi, fotoğrafı, eğitim bilgileri, parmak izi, sağlık bilgileri, kurum sicili, emeklilik bilgileri, sosyal medyada yazdığı yayımladığı her türlü yazı, fotoğraf, ses ve görüntü kayıtları vb. veriler kişisel veri olarak kabul edilebilir.

Kurumsal bilgi güvenliği, kurumların bilgi varlıklarının güvenlik zafiyetleri belirlenerek bu varlıkların kendisine yönelik her türlü arzu edilmeyen tehdit ve saldırılardan korunması için gerekli olan güvenlik altyapılarının oluşturularak tedbirlerin alınması şeklinde tanımlanabilir. Kurumsal bilgi güvenliği, sistem, teknoloji, insan, eğitim gibi pek çok faktörü tek çatı altında toplayarak yönetilmesi zor bir süreçtir. Bu sürecin yönetilmesinde güvenlik sistem ve politikalarının uluslararası standartlarda yönetilmesi ve yapılandırılmasına yönelik tüm dünyada kurumsal bilgi güvenliğinin standartlaştırılması yönünde çalışmalar yapılmaktadır (Baykara, Daş ve Karadoğan, 2013). Ulusal bilgi güvenliği bir organizasyon ya da kurumun kurumsal bilgi güvenliği çalışmalarından çok daha kapsamlı olup kurumsal bilgi güvenliğinin sağlanmasındaki gerekliliklerle birlikte uluslararası işbirliği, siber suçlarla mücadele, kamu- özel işbirliği, ulusal güvenlik gibi kavramları da bünyesinde toplamaktadır (Güngör, 2015).

Bilgi Güvenliğinin Kapsamı

Bilgi güvenliği kişisel bilgisayar ve mobil cihazlardan başlayarak kurumsal ve ulusal çaptaki tüm iletişim cihazlarını ve kritik bilgi altyapılarını da kapsayan geniş bir çerçevede bilgi sistemlerinin dahil olduğu güvenlik yönetimi anlayışı olarak tanımlanmaktadır (Güngör, 2015). Bu güvenlik yönetimi anlayışı sayısal ortamda saklanan verinin göndericiden alıcıya bütünlüğü ve doğruluğu bozulmadan taşınması, saklanan veriye her an güvenli bir şekilde erişilmesi ve bilginin izinsiz ve yetkisiz erişimlerden korunması için gerekli tüm çalışmalardır. Bu anlayış çerçevesinde bilgi güvenliği yönetim politikaları oluşturulmalı ve uygulanmalıdır. Bu politikalar bilginin gerekli ve yeteri kadar erişimine izin vermeli, bilginin silinmesi işlemlerini sınırlandırılmalı ve yapılan bütün işlemler için sağlıklı log kayıtlarına olanak sağlamalıdır.

Kritik altyapılar bilgi güvenliği açısından büyük öneme sahiptir (Şekil 2). Genel geçer bir kritik altyapı tanımı olmamakla birlikte nerede kullanıldığına göre ülkeler ya da kurumlar bazında çeşitli tanımlamalar yapılmaktadır. Kullanıldığı yer ve duruma göre tanımlar farklılık gösterse de ortak özellikleri ele alındığında işlevlerini kısmen veya tamamen, yerine getirmediğinde, kurum düzeninin ya da toplumsal düzenin sürdürülebilirliğinin kesintiye uğrayabileceği ve/veya kamu hizmetlerinin verilmesinde olumsuzluklar yaşanacağı tüm ağ, varlık, yapı ve sistemlerin tamamı olarak kısaca tanımlamak mümkündür.



Şekil 2. Kritik altyapı sektörleri (Güngör, 2015)

Bilgi Güvenliğinin Amacı

Bilgi güvenliği, bilgi sistemlerinin işleyişinin kesintisiz, kaliteli ve güvenilir bir şekilde devam ettirilmesini sağlamaktır. Böylece kurum ve ülke imajının zedelenmemesi güvenliğin sağlanması ile bilgi varlıklarının korunması ve yetkisiz kişilerin erişiminin engellenmesidir.

Bilgi Güvenliğinin Konusu

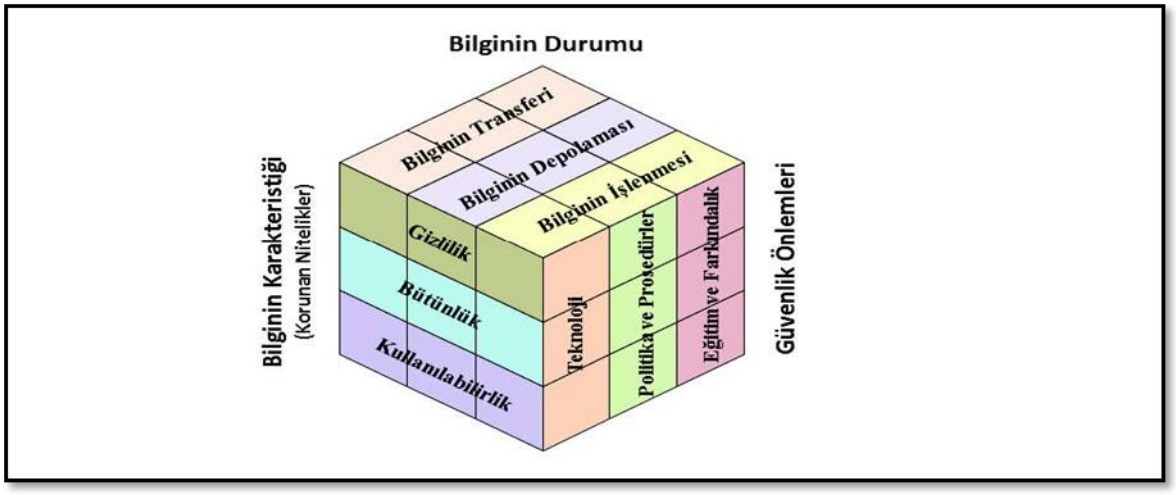
Bilgi güvenliğinin temeli bilginin gizlilik, bütünlük ve kullanılabilirliğine yönelik her türlü saldırı ve tehditlere karşı korumak ve bu tehditlerin yararlanabileceği güvenlik açıklarının belirleyerek önlem almaktır. İlk bakışta basit ve anlaşılır görünse de tehdit ve saldırıların çeşitlenmesi, çoğalması ve karmaşıklaşması sebebiyle bilgi güvenliğini sağlamak giderek zorlaşmaktadır.

Bilgi Güvenliği Unsurları

Bilgi güvenliğinin sürekli korunması gereken nitelikleri bir diğer ifadeyle korunması gereken ilkeleri bulunmaktadır. Bilgi güvenliği Solomon'un (Solomon ve Chapple, 2005) bilgi güvenliği üçgeninde anlattığı gibi gizlilik, bütünlük ve erişilebilirlik olmak üzere bu üç unsurun bileşimi kabul edilmekte ve bu üç unsur üzerine kurulmaktadır.

Şekil 3'te gösterilen McCumber Bilgi Güvenliği modeli bilgi güvenliği alanında hem ulusal hem de uluslararası boyutta bilgi güvenliği politikası geliştirebilmek ve bilgi güvenliğini gerçekten tüm

yönleriyle ele alabilmek için temel alınabilecek en uygun ve anlamlı modellerden biridir. Bilgi güvenliğini tüm unsurlarıyla birlikte farklı boyutlarda gruplandırarak gösteren McCumber modeli 1991' den beri geçerliliğini korumuş ve diğer geliştirilen modellerde temel kabul edilerek yol gösterici olmuştur. McCumber bu modeline göre bilgi güvenliği politikaları oluşturulurken ve uygulamaya dönüştürülürken tüm yönleri ile birlikte ele alınmadığı sürece bilgi güvenliğinin sağlanması ve bilgi güvenliği politikalarının başarıya ulaşması mümkün değildir.



Şekil 3. McCumber bilgi güvenliği modeli (McCumber,1991)

Bilginin gizliliği, bütünlüğü, erişilebilirliği kadar bilgi güvenliği sürecinde etkili olan bilgi güvenliği politika ve prosedürlerinin ve insan faktörünün büyük önemi bulunmaktadır. Bilgi güvenliği politikalarını olabilecek en iyi ve katı ve kapsamlı kurallarla uygulayan kuruluşlar da McCumber bilgi modeline temel bilgi güvenliği kavramları içerisinde yer ayırmaktadır (Öğün ve Kaya, 2013).

Bilgi güvenliği politikalarına farklı açılardan ve detaylı bir perspektiften bakmayı sağlayan McCumber modeli, kurumlar için bilgi güvenliği politika ve prosedürlerini oluştururken dikkate alınması gereken önemli bir modeldir. Modelde bilgi güvenliğinin farklı boyutlarını gösteren gruplar yer almaktadır. Bir yüzünde bilgi güvenliğinin temel unsurları olarak kabul edilen gizlilik, bütünlük ve kullanılabilirlik ilkeleri bilginin karakteristiği adı altında toplanmıştır. Diğer yüzde ise bilginin transferi, bilginin depolanması ve bilginin işlenmesi işlemleri bilginin durumu ismiyle gruplandırılmıştır. Küpün üçüncü ve son yüzünde ise teknoloji, politika ve prosedürler ile eğitim ve farkındalık alanları güvenlik önlemleri başlığı altında toplanmıştır.

BİLGİ GÜVENLİĞİNİ TEHDİT EDEN UNSURLAR

İnternetin hayatımıza girmesiyle birlikte internet kullanıcı sayısı müthiş bir şekilde artmaktadır. Dünya nüfusunun yarısından fazlası internet ve mobil cihaz kullanmakta iken yarısına yakını sosyal medya kullanmaktadır. Türkiye' de ise durum farklı değildir. Türkiye İstatistik Kurumunun 2018 yılında yayınladığı TÜİK Bilgi Toplumu İstatistikleri Raporuna göre ülkemizde bir önceki yıla göre internet kullanıcı oranı artarak %80,7 olarak açıklamıştır. Yine aynı rapora göre web sitesi sahipliği oranı ise %72,9 olarak raporlanmıştır.

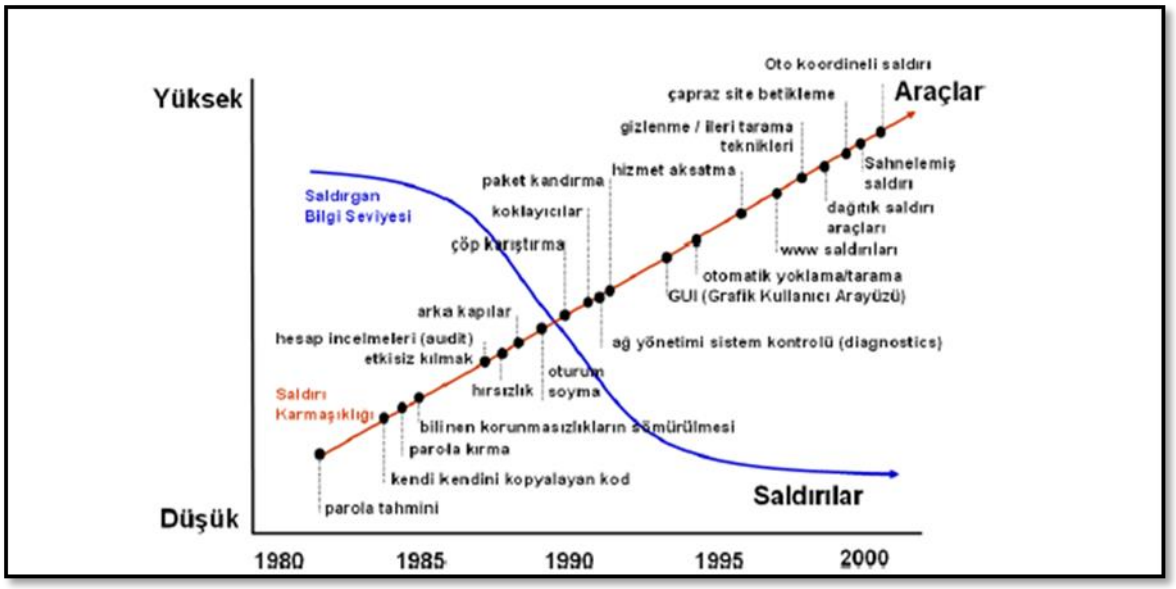
Türkiye ve Dünyada internet kullanım rakamlarına bakıldığında internetin hayatımızda ne kadar yer aldığı anlaşılmaktadır. İnternetin sağladığı pek çok kolaylık, rahatlık ve avantajın yanında çeşitli güvenlik sorununu da beraberinde getirmektedir. Bu durum kullanıcılar için birçok risk ortaya çıkarmıştır.

İnternetin kullanılmasıyla ortaya çıkan riskler kullanıcıyı hem ruhsal hem de fiziksel yönden etkilediği gibi, maddi ve sosyal açıdan zarar da verebilmektedir. Bu riskler saldırı, atak veya tehdit olarak adlandırılmaktadır. Kısaca bilgi veya bilgisayar güvenliğinde kötü niyetli kişiler tarafından yapılan saldırılardır. Bilgi sistemini geçmek veya aldatmak, zayıflıklarını kullanmak, kişilere veya sistemlere

direkt olarak veya dolaylı olarak zarar vermek, sistemlerin sürdürülebilirliğini bozmak, durdurmak, işlemez hale getirmek gibi kötü amaçlarla yapılan eylemler saldırı veya atak olarak isimlendirilmektedir (Canbek ve Sağıroğlu, 2006). Bu kötü niyetli kişiler amaçlarına ulaşabilmek için çok çeşitli yöntemlerle saldırılar gerçekleştirmektedirler. Kötü niyetli kişiler olarak tanımlanan aslında bilgisayar korsanları olarak da adlandırılmaktadır.

Bilgi Güvenliğine Yönelik Tehdit Çeşitleri

Basit düzeyde başlayan kötü niyetli ve kötücül saldırılar zaman içerisinde daha çok çeşitlenip artarak devam etmiştir. Şekil 4'te görüldüğü gibi teknoloji geliştikçe saldırılar da farklılıklar göstermektedir. İlk zamanlar kurumlarda notların yazıldığı kağıt çöplerini karıştırma ve parola tahmin etme gibi basit saldırıların yerini günümüzde çapraz site betikleme (cross site scripting), dağıtık hizmet engelleme saldırıları (distributed denial of service), oto koordineli saldırı (auto coordinated attack), hizmet aksatma (denial of service) ve sahnelenmiş saldırılar (staged attacks) gibi çok daha karmaşık ve kapsamlı, çok daha detaylı, çok daha anlaşılması zor ve önlem alınması uğraştırıcı ve maliyetli saldırılar almıştır.



Şekil 4. Saldırı karmaşıklığı ve saldırgan teknik bilgisi (Canbek ve Sağıroğlu, 2006)

Vural (2007), tehditlerin bilgi sistemlerinde etkili olabilmek için sistem açıklarını kullandıklarını ve bilgi varlıklarına etkilerinin tehlikenin gerçekleşme olasılığı sistemdeki açık miktarı ve bilginin değerine göre değiştiği bilgisi üzerinde durmuştur. Böylece tıpkı vücudumuza girmeyi bekleyen virüs ve bakteriler gibi bağışıklığın çöktüğü an ya da açık verdiği an etkili olmakta tıpkı bunun gibi bilgi sistemlerindeki güvenlik açığı fark edildiği an bilgi sistemlerine zarar vermektedir. Tehditlerin bilgisayar sistemlerine zarar verecek düzeye gelmesinde en önemli etken teknik ve bireysel zafiyetlerdir.

TEHDİTLERE KARŞI ALINMASI GEREKEN ÖNLEMLER

Genel olarak bilgi güvenliğini sağlamak için öncelikle en küçük birimin yani bireyin alması gereken kişisel veri güvenliği önlemlerini daha önceki yapılmış çalışmalardan aşağıdaki şekilde özetlemek mümkündür (Karakoç, 2011; Yavanoğlu ve Sağıroğlu, 2012).

- Web sayfalarında istemsiz olarak açılan pencerelerin kapatılması,
- Web sayfalarında güvenlik sertifikalarının kontrol edilmesi,
- Bilgisayarda güncel güvenlik yazılımının bulundurulması,
- Lisanslı işletim sistemleri ve lisanslı yazılımların kullanılması,
- Bilgisayarda kullanılan yazılımların (özellikle antivirüs ve işletim sistemi) güncel olması,
- Farklı amaçlar için kullanılan şifrelerin (yani internet alışveriş siteleri, banka şifreleri,

bilgisayar açılış şifresi, vb.) birbirinden bağımsız olması, farklı simge, rakam, karakter içermesi ve en az 8 karakterden oluşması,
- Şifre hatırlatma için kullanılan gizli soruların ve yanıtlarının zor olması,
- Bilgisayarda yer alan önemli olduğu düşünülen dosyaların güvenli bir ortama yedeklerinin alınması,
- Güvenli olmayan ve kaynağı bilinmeyen e-postaların açılmadan silinmesi,
- E-postalarda gelen bilinmeyen web sayfalarına giriş işlemi yapılmaması,
- Şifreli işlemlerde sayfadan 'Oturumu Kapat' komutuyla çıkılması,
- Kablosuz ağ modemlerinin şifresiz kullanılmaması (fakat kolay şifreler de belirlenmemeli Örn:12345),
- Kablosuz internet modemlerinin parolalarının belirli aralıklarla değiştirilmesi,
- Sosyal paylaşım sitelerinde kişisel bilgilerin paylaşılmaması,
- Sosyal paylaşım sitelerinde mümkün olduğunca özel olan fotoğraf, video gibi medyaların paylaşılmaması,
- Sosyal ağlarda mümkün olduğunca ve gerekmedikçe yer bildirimi yapılmaması,
- Sosyal paylaşım sitelerinde yabancı kişilerden gönderilen arkadaşlık isteklerinde dikkatli davranılması,
- Sosyal paylaşım ağlarından veya e-posta yoluyla gelen para, kontör, vb. isteklerin dikkate alınmaması,
- Sosyal paylaşım veya sohbet sitelerinde yabancı kişiler ile görüntülü, sesli ve hatta gerçek hayatta yüz yüze iletişime geçilmemesi,
- Bankacılık ve çevrimiçi alışveriş işlemlerinin ortak alan bilgisayarlarından yapılmaması,
- Çevrimiçi alışveriş işlemlerinde düşük limiti sanal kartlar kullanılması,
- İnternet üzerinden tehdit, şantaj veya cinsel istismara maruz kalma durumlarında hukuksal yönlerinin öğrenilerek bu yollara başvurulması

olarak sıralamak mümkündür.

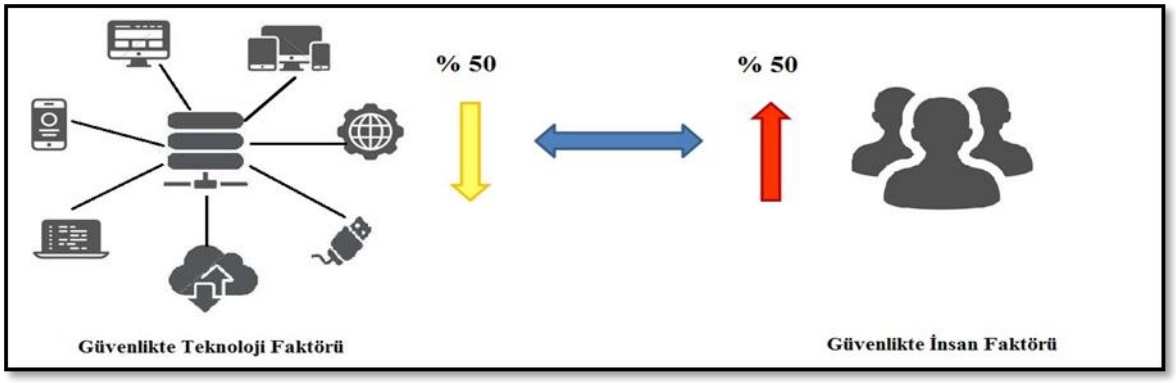
Kişilerin bilgi güvenliği kadar kişilerin bilgi güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğini de sağlamak da önemlidir. Kurumsal bilgi güvenliğini sağlamak için çok çeşitli teknolojiler kullanılmaktadır. Bu sistemler güvenlik duvarları, dıştan içe saldırı tespit sistemleri ve içten dışa saldırı sistemleri olarak sıralanabilir. Ağlar arasında taşınan verinin bütünlüğü ve gizliliğini sağlamak için kimlik doğrulama ve gönderilen verilerinin şifrelenmesi tercih edilmektedir. Ayrıca yukarıda sayılan kişisel bilgi güvenliği önlemlerine ek olarak kurum personeli tarafından uygulandığında kurum bilgi güvenliğine katkı sağlayacak bazı önlemler bulunmaktadır. Bunlar;

- Kötücül yazılımlardan koruma programlarının ve işletim sistemlerinin güncellemelerinin düzenli olarak yapılması,
- Bilgisayara kurulan yazılımların paylaşıma açık olup olmadığına dikkat edilmesi,
- Bilgisayar ekranlarının şifreli ekran koruyucularla korunması,
- Bilgisayarda işlem yapılmayan sürelerde ekranı kilitlemeden ayrılmaması,
- Bilgisayar başından uzun süre ayrı kalındığında kurum bilgi sistemlerinden çıkış yapılması,
- Disk ve dosya paylaşımlarında dikkatli olunması,
- Önemli dokümanların parola koyularak korunması veya şifrelenerek saklanması,
- Gizli ve önemli bilgilerin güvenli olan yollardan gönderilmesi,
- Önemli bilgi içeren belge ve dosyaların düzenli olarak yedeklenmesi

olarak sayılabilir.

Yukarıda sayılan güvenlik tedbirleri hem bireysel hem de kurumsal olarak uygulandığında önemli derecede başarılar elde edilmesine rağmen bu yöntemlerin etkinliği insan faktörünün devreye girmesiyle zafiyete uğramaktadır (Şekil 5). Bu önlem ve tedbirlerin pek çoğu bilgisayar virüsleri, aldatmacalar, yetkisiz erişim, siber dolandırıcılık, bilgi hırsızlığı gibi teknoloji kaynaklı riskler ve tehditler için uygulandığında önemli ölçüde etkili olacak tedbirlerdir. Tüm bu tedbirlere rağmen sistemin kullananının insan olması unutulmamalıdır. Bazen kötü niyet taşımadan bilinçsizce yapılan bir işlem dahi ciddi tehlikeler oluşturmaktadır. Kurumlar teknolojik olarak güvenlik önlemlerini alsa

dahi insan kaynaklı tehditleri de göz ardı etmemek durumundadır. Bu noktadan hareketle güvenlik tehditlerini en aza indirmenin yollarından birisi de farkındalık oluşturmaktır.



Şekil 5. Güvenlikte insan faktörü (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009)

Bilgi güvenliği üzerine yapılan çalışmalarda insan ve teknoloji faktörünün aynı oranda etkili olduğu görülmektedir. Bu durum bilgi güvenliği bilinci ve farkındalık düzeyinin yüksekliğinin kişisel veri güvenliği yanında kurumsal bilgi güvenliğini de sağladığını göstermektedir. Kurumsal bilgi güvenliğinin sağlanması da ulusal siber güvenliği getirecektir.

Farkındalık

Farkındalık sözcüğü Türk Dil Kurumu (TDK) sözlüğünde *"farkında olma durumu"* olarak ifade edilmektedir. Farkında olmak ise "görülmesi veya bilinmesi gereken şeylerden haberi bulunmak, kavranması gereken bir şeye dikkat etmek" şeklinde tanımlanmaktadır (TDK, 2019).

Kurumsal bilgi güvenliği farkındalığı

Kurumsal bilgi güvenliği farkındalığı sağlamak için üst düzey yöneticiden çalışana kadar bilgilendirilmesi, farkındalık bilincinin oluşturulması, güvenlik politikalarının benimsenmesi, önemsenmesi, desteklenmesi ve birlikte geliştirilmesi gerekmektedir.

İnsan faktörüne bağlı olarak ortaya çıkan güvenlik risklerinin tamamen yok edilmesi mümkün değildir ancak iyi planlanmış bir bilgi güvenliği politikası ve bu politikayı uygulamak için kararlı, bilgili ve farkındalık düzeyi yüksek çalışanlar ile bu risklerin kabul edilebilir seviyelere düşmesi sağlanabilir.

Kurumsal bilgi güvenliğinden sadece kurumun bilgi güvenliği personeli ya da teknik çalışanlar değil kurumun tüm çalışanları, bilgi paylaşımında bulunduğu tüm paydaşları yani kurum bilgi güvenliği politikasında bulunan taraflar sorumludur. Bu sorumluluk bilincinin bilgi güvenliği farkındalık eğitimleri ile tüm çalışanlara verilmesi, hangi tür risklerle karşılaşabilecekleri ve bu sorunlar karşısında nasıl tedbirler almaları ve davranmaları gerektiği anlatılmalıdır.

Bilgi Güvenliği Farkındalığı Oluşturma Önerileri

Günümüz koşullarında kurumun esas değerini oluşturan insan varlığıdır. Kurum politikası olarak insan varlığına yatırım yapıldığında aslında kuruma yatırım yapıldığıdır. Kurum çalışanlarında bilgi güvenliği farkındalığı oluşturmak için öncelikle yöneticilerin farkındalık çalışmalarını sahiplenmesi ve gerekliliğini inanması gerekmektedir. Sonrasında bu konuda personele eğitim vermek bilgi güvenliği personeline bırakılmalıdır. Eğer bu konuda bilgi güvenliği çalışanları yeterli bilgi donanımına sahip değilse danışmanlık hizmeti alınmalıdır (Şahinaslan ve arkadaşları, 2009)

BİLGİ GÜVENLİĞİ FARKINDALIĞI ÜZERİNE YAPILAN YURT İÇİ ve YURT DIŞI ÇALIŞMALAR

Bilgi güvenliği farkındalığı bireylerin bilgi iletişim teknolojileri kullanımında, kişisel verileri bilgi güvenliğine karşı oluşabilecek risk ve tehlikelerden korumak için gerekli güvenlik tedbirlerini

uygulamak ve bu tehditlerin farkında olması durumudur (Vural ve Sağıroğlu, 2008). Bu sebeple bu konuda bilgi güvenliği eğitimiyle alakalı yapılan ulusal ve uluslararası çalışmaları incelemek gerekmektedir. Bilgi güvenliği ile ilgili araştırmaların yapılması, hem internet ve bilgisayar olmak üzere siber alan kullanıcılarının hem de bu konuda eğitim verecek olanlara yol göstermesi açısından önemlidir. Bilgi güvenliği farkındalık boyutunu inceleyen araştırma çalışmalarında genellikle veri toplama aracı olarak yüz yüze görüşme, anket veya ölçek kullanılmıştır.

Alanyazında bilgi güvenliğinin sağlanmasına yönelik oldukça çalışma bulunmaktadır. Ancak McCumber Bilgi Güvenliği Modelinde kabul edildiği gibi küpün tamamlayıcı niteliklere sahip yüzünde yer alan Eğitim ve Farkındalık yani insanın dâhil olduğu alanın öneminin son yıllarda keşfedildiği görülmektedir.

Herath ve Rao (2009), çalışma alanlarını biraz daha değiştirerek bilgi güvenliği politikalarına uyma niyetleri gibi insan davranışlarını incelemişlerdir. Ancak bu çalışma ne kadar bilgi güvenliğine etkisi olan güvenlik politikaların davranışların etkisini incelese de bilgi güvenliği farkındalığını belirlemeye yönelik bir çalışma değildir.

Ünver, Canbay ve Mirzaoğlu (2009),araştırmalarında daha çok bilgi güvenliği zafiyetlerine üzerinde durmuştur. İnternet üzerinden yapılan işlemlerin çoğunda kimlik numarasının kullanılması ve kimlik numarasından bütün kişisel bilgilere ulaşılmasından dolayı oluşan tehlikelerden bahsetmişlerdir.

Lao ve arkadaşları (2009) tarafından yapılan çalışmada özellikle sosyal ağlarda yayılan ve kullanıcılar tarafından fark edilmeyen tehditler üzerinde durulmuştur. Bu tehditlerin kullanıcıları ve sosyal paylaşım sitelerini nasıl etkilediği ayrı ayrı anlatılmış ve bu tehditlere karşı alınabilecek olan önlemler ile sosyal ağlar için özel bir güvenlik arabirimi önerilmiştir. Aynı zamanda kullanıcıların farkındalığının yükseltilmesi önerisinde de bulunulmuştur.

Vroom ve vonSolms (2004) tarafından yapılan araştırmada bilgi güvenliği farkındalığının oluşmasında bilgi güvenliği politikalarının, kurumsal olarak yapılan bilgilendirme çalışmalarının, kişisel özellikler de dahil olmak üzere kurum kültürü gibi etmenlerin dahi bilgi güvenliği farkındalığı oluşturulmasında etkili olduğu ifade edilmiştir.

Tekerek ve Tekerek (2013) tarafından yapılan çalışmada Kahramanmaraş ilindeki ilk ve orta öğretim öğrencilerine bilgi güvenliği farkındalık seviyelerini belirlemek amacıyla geliştirdikleri ölçeği uygulamışlardır. Araştırma sonucu öğrencilerin etik konularda yeterli düzeyde farkındalıklarının olduğu ancak teknik konularda farkındalıklarının düşük olduğu yönündedir. Bunun sebebi olarak bilgi ve bilgisayar güvenliği farkındalık eğitim ve etkinliklerinin yetersiz olması gösterilmiş, bu konudaki eğitimlerin artırılması yönünde öneride bulunulmuştur.

Kınay, Sözcü, Taşkın ve İpek (2014) tarafından geliştirilen Bilgi Güvenliği Farkındalığı Ölçeği, İstanbul ilinde özel bir üniversitenin öğrencilerine uygulanmıştır. Ölçekte eğitim, bilgi ve davranış düzeylerinde 32 soru bulunmaktadır. Ölçekten elde edilen puanlar 100-80 arası 'yüksek', 79-60 arası 'orta', 60 ve aşağısı ise düşük seviye olarak belirlenmiştir. Her farkındalık seviyesi için alınması gereken kararlar tartışılmıştır.

Araştırmalar arasında en dikkat çekici olanı 2000-2009 yılları arasında Tayvan' da devlet desteğiyle uygulanan İnternet Güvenliğinde Öğretmen Farkındalığı (TAIS) projesidir. Tayvan Milli Eğitim Bakanlığı internetin risklerinin farkına vararak ada çapında ilk ve ortaokul öğretmenlerine yönelik hazırladığı projede araştırmacılar internet güvenliğini öğretmenlerin fikir sahibi oldukları dört alan üzerinden gerçekleştirmiştir. Bu alanlar iletişim güvenliği, bilgi anlayışı ve uygunluk, çevrimiçi kişiler arası güvenlik, bilgisayar ve internet kullanımı güvenliğidir. Üç aşamalı olan projenin ilk aşamasında yalnızca bilgisayar öğretmenleri dahil olurken ikinci aşamasında tüm ilk ve ortaokul öğretmenleri dahil edilmiştir. Ancak projenin son aşaması olan veliler, lise öğrencileri, lise öğretmenleri ve öğretmen adayları projeye dâhil edilememiştir. Proje kapsamında eğitim seminerleri, atölye çalışmaları, konferanslar gibi çeşitli etkinlikler yer almıştır.

Bilgi güvenliğinin sağlanmasında donanım ve yazılım destekli tedbirler alınmaya ve bilgi güvenliği politikaları oluşturulmaya çalışılsa da en zayıf halkanın insan faktörü olduğu unutulmamalıdır. Eminağaoğlu ve Gökşen (2009), çalışmasında bilgi güvenliğinde başarı sağlanmasındaki en kritik faktörün bilinçli ve bilgili insanlar olduğunu vurgulamaktadır. Geliştirilen donanım ve yazılımları bilgi

güvenliği hakkında bilgisi olan kullanıcılar bilinçli olarak kullandığında veri kayıplarının ve zararın çoğu önlenebilir. Şahinaslan ve arkadaşları (2009) yaptığı çalışmasında kurumlarda bilgi güvenliğini sağlamak amacıyla sadece teknik önlemlerin alınmasının yeterli olmayacağını en önemli faktörün insan olduğunu ve bilgi güvenliği risklerinin önlenmesinin ancak farkındalık düzeyinin artırılmasıyla mümkün olacağını belirtmiştir.

Çalışmanın Amacı ve Araştırma Problemleri

Bu araştırmanın amacı kamu kurum çalışanlarının siber saldırılar karşısında bilgi güvenliği farkındalık seviyeleri ölçmektir. Bu amaç doğrultusunda aşağıda sıralanan alt problemlere cevap aranmıştır:

1. Kamu çalışanlarının bilgi güvenliği farkındalığı cinsiyete göre anlamlı farklılık göstermekte midir?
2. Kamu çalışanlarının bilgi güvenliği farkındalığı yaş aralığına göre anlamlı farklılık göstermekte midir?
3. Kamu çalışanlarının bilgi güvenliği farkındalığı eğitim düzeyine göre anlamlı farklılık göstermekte midir?
4. Kamu çalışanlarının bilgi güvenliği farkındalığı görev yapılan birime göre anlamlı farklılık göstermekte midir?

METODOLOJİ

Çalışmada nicel araştırma modellerinden betimsel tarama yöntemi kullanılmıştır. King ve He (2005) betimsel tarama yöntemini nicel bir yaklaşım olarak ifade etmektedir. Betimsel tarama, grupların herhangi bir olgu ya da konu ile ilgili görüşlerinin betimlendiği araştırmalardır. Bu araştırmada veri toplama aşamasından önce Gazi Üniversitesi Ölçme Değerlendirme Etik Alt Çalışma Grubu'ndan 91610558-302.08.01- sayılı kararı ile (Araştırma kod no: 2019-243) gerekli izinler alınmıştır.

Katılımcılar

Araştırmaya 302 erkek (%60,3) ve 199 (%39,7) kadın katılmıştır. Katılımcıların 59'u (%11,8) 20-30 yaş aralığında, 211'i (%42,1) 31-40 yaş aralığında, 159'u (%31,7) 41-50 yaş aralığında ve 72'si (%14,4) 51-70 yaş aralığındadır. Katılımcıların büyük çoğunluğu üniversite mezunu olup (%89,4), 72'si (%85,6) Bilgi Teknolojileri Daire Başkanlığında, 429'u (%85,6) ise destek veren kurum ve kuruluşların diğer birimlerinde görev yapmaktadır.

Veri Toplama Araçları

Araştırmada Keser ve Güldüren (2015) tarafından geliştirilen Bilgi Güvenliği Farkındalık Ölçeği kullanılmıştır. Ölçek 'Kişisel Verilerin Korunması' ve 'Saldırı ve Tehditler' olmak üzere iki alt faktör ve 34 sorudan oluşmaktadır. Ölçeğin tamamı için Cronbach alfa güvenilirlik katsayısı .97'dir. Bu çalışmada Cronbach alfa güvenirlik katsayıları "Saldırı ve Tehditler" alt boyutu için .96; "Kişisel Verilerin Korunması" alt boyutu için .96; ölçeğin tümü içinse .97 olarak hesaplanmıştır.

Verilerin Analizi

Araştırmada bilgi güvenliği farkındalığı toplam puanları cinsiyete, yaş aralığına, eğitim düzeylerine ve çalışılan birime göre karşılaştırılmış, cinsiyete, çalışılan birime, eğitim düzeylerine ve yaş aralığına göre ortalamalar belirlenerek gruplar arası karşılaştırmalar yapılmıştır.

Bulgular

Bu bölümde araştırma kapsamında ulaşılan bulgulara yer verilmiştir. Katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin "Saldırı ve Tehditler" ile "Kişisel Verilerin Korunması" alt boyutlarından ve ölçeğin toplamından elde ettikleri puanların cinsiyetlerine, yaşlarına, eğitim düzeylerine ve çalıştıkları birime göre karşılaştırma sonuçları sunulmuştur.

<u>Cinsiyet ve Bilgi Güvenliği Farkındalığı</u>

Katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin "Saldırı ve Tehditler" ile "Kişisel Verilerin Korunması" alt boyutlarından ve ölçeğin toplamından elde ettikleri puanların cinsiyetlerine göre

farklılaşıp farklılaşmadığının belirlenmesi amacıyla bağımsız gruplar için t-testi yapılmıştır. Yapılan karşılaştırmalarda, hem alt boyutlar hem de ölçeğin tümü için, kadın ve erkek katılımcıların ortalama puanları belirlenmiş, ortalama puanlar arasında farkın anlamlılığının testi içinse t değeri hesaplanmıştır. Bulgular ölçeğin tümü için aşağıda Tablo 1'de sunulmuştur.

Tablo 1. Katılımcıların bilgi güvenliği farkındalığı ölçeğinden elde ettikleri toplam puanların cinsiyetlerine göre karşılaştırılması

Cinsiyet	N	Ort	Ss	Sd	*t*	p
Kadın	302	110,00	31,08	499	1,952	,052
Erkek	199	104,64	28,43			

Tablo 1 incelendiğinde, kadın katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin toplamından elde ettikleri puan ortalamalarının 110,00 (ss=31,08) olduğu, erkek katılımcıların elde ettikleri puan ortalamalarının 104,64 (ss=28,43) olduğu görülmektedir. Puan ortalamalarının karşılaştırılması sonucunda ise, kadın ve erkek katılımcılarının ortalama puanlarının birbirinden anlamlı olarak farklılaşmadığı bulunmuştur (t(499)= 1,952; p> ,05). Bir başka deyişle, genel olarak kadın ve erkek katılımcılar benzer düzeyde bilgi güvenliği farkındalığına sahiptirler.

Yaş ve Bilgi Güvenliği Farkındalığı

Katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin "Saldırı ve Tehditler" ile "Kişisel Verilerin Korunması" alt boyutlarından ve ölçeğin toplamından elde ettikleri puanların yaş aralıklarına göre farklılaşıp farklılaşmadığının belirlenmesi amacıyla tek yönlü varyans analizi (ANOVA) yapılmıştır. Yapılan karşılaştırmalarda, hem alt boyutlar hem de ölçeğin tümü için, yaş aralıklarına göre katılımcıların ortalama puanları belirlenmiş, ortalama puanlar arasındaki farkın anlamlılığının ortaya konulması amacıyla Tukey testi yapılmıştır. Bulgular ölçeğin tümü için Tablo 2'de sunulmuştur.

Tablo 2. Katılımcıların bilgi güvenliği farkındalığı ölçeğinden elde ettikleri toplam puan ortalamalarının yaş aralıklarına göre dağılımı

Yaş Aralığı	N	Ort.	Ss
20-30 Yaş	59	110,74	27,47
31-40 Yaş	211	114,18	29,54
41-50 Yaş	159	103,34	29,10
51-70 Yaş	72	97,01	32,00

Tablo 2 incelendiğinde Bilgi Güvenliği Farkındalığı Ölçeğinin toplamı için 20-30 yaş aralığındaki katılımcıların puan ortalamalarının 110,74 (ss=27,47); 31-40 yaş aralığındaki katılımcıların puan ortalamalarının 114,18 (ss=29,54); 41-50 yaş aralığındaki katılımcıların puan ortalamalarının 103,34 (ss=29,10); 51-70 yaş aralığındaki katılımcıların puan ortalamalarının ise 97,01 (ss=32,00) olduğu görülmektedir. 31-40 yaş aralığındaki katılımcılar en yüksek puan ortalamasına sahip iken 51-70 yaş aralığındaki katılımcılar en düşük puan ortalamasına sahiptir. Puan ortalamaları arasındaki farkın anlamlı olup olmadığının belirlenmesi amacıyla yapılan tek yönlü varyans analizi sonuçları Tablo 3'te sunulmuştur.

Tablo 3. Katılımcıların bilgi güvenliği farkındalığı ölçeğinden elde ettikleri toplam puanların yaş aralıklarına göre karşılaştırılması

	Kareler Toplamı	Sd	Kareler Ortalaması	F	p
Gruplar Arası	20641,885	3	6880,628	7,887	,000
Grup İçi	433605,939	497	872,447		
Toplam	454247,824	500			

Tablo 3 incelendiğinde katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinden elde ettikleri toplam puanların ortalamalarının yaş aralıklarına göre anlamlı olarak farklılaştığı görülmektedir ($F(497)=7,887$; $p< ,05$). Çizelge 12 gruplar arasında farkın olduğunu söylemekle birlikte, hangi gruplar arasında bu farkın olduğunu bildirmemektedir. Hangi yaş grupları arasında anlamlı farklılığın olduğunu belirlemek amacıyla ise Tukey testi yapılmıştır. Tukey testi sonuçlarına göre, 31-40 yaş aralığındaki katılımcıların hem 41-50 yaş aralığındaki hem de 51-70 yaş aralığındaki katılımcılardan anlamlı olarak daha yüksek puan aldıkları bulunmuştur. Ek olarak, 21-30 yaş aralığındaki katılımcılar 51-70 yaş aralığındaki katılımcılar anlamlı olarak daha yüksek puan almışlardır.

Bilgi Güvenliği Farkındalığı ve Eğitim Düzeyi

Katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin "Saldırı ve Tehditler" ile "Kişisel Verilerin Korunması" alt boyutlarından ve ölçeğin toplamından elde ettikleri puanların eğitim düzeylerine göre farklılaşıp farklılaşmadığının belirlenmesi amacıyla bağımsız gruplar için t-testi yapılmıştır. Lise ve altı eğitim düzeyine sahip katılımcılar bir grup, üniversite mezuniyetine sahip katılımcılar ise diğer bir grup olarak ele alınmıştır. Yapılan karşılaştırmalarda, hem alt boyutlar hem de ölçeğin tümü için, katılımcıların eğitim düzeylerine göre ortalama puanları belirlenmiş, ortalama puanlar arasında farkın anlamlılığının testi içinse t değeri hesaplanmıştır. Bulgular ölçeğin tümü için Tablo 4'te sunulmuştur.

Tablo 4. Katılımcıların bilgi güvenliği farkındalığı ölçeğinden elde ettikleri toplam puanların eğitim düzeylerine göre karşılaştırılması

Eğitim Düzeyi	N	Ort	Ss	Sd	*t*	p
Lise ve Altı	53	90,87	31,90	496	-4,505	,000
Üniversite	445	110,14	29,15			

Tablo 4 incelendiğinde, lise ve altı eğitim düzeyine sahip katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin toplamından elde ettikleri puan ortalamalarının 90,87 (ss=31,90) olduğu, üniversite mezunu katılımcıların elde ettikleri puan ortalamalarının 110,14 (ss=29,15) olduğu görülmektedir. Puan ortalamalarının karşılaştırılması sonucunda ise, üniversite mezunu katılımcıların ortalama puanlarının anlamlı olarak daha yüksek olduğu bulunmuştur ($t(496)= -4,505$; $p< ,05$). Bir başka deyişle, üniversite mezunu katılımcılar bilgi güvenliği konusunda lise ve altı eğitim düzeyine sahip katılımcılara oranla daha yüksek farkındalığına sahiptirler.

Bilgi Güvenliği Farkındalığı ve Görev Yapılan Birim

Katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin "Saldırı ve Tehditler" ile "Kişisel Verilerin Korunması" alt boyutlarından ve ölçeğin toplamından elde ettikleri puanların görev yaptıkları birime göre farklılaşıp farklılaşmadığının belirlenmesi amacıyla bağımsız gruplar için t-testi yapılmıştır. Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcılar bir grup olarak ele alınırken, diğer tüm birimlerde görev yapan katılımcılar ise "diğer" olarak ele alınmıştır. Yapılan karşılaştırmalarda, hem alt boyutlar hem de ölçeğin tümü için, katılımcıların çalıştıkları birime göre ortalama puanları belirlenmiş, ortalama puanlar arasında farkın anlamlılığının testi içinse t değeri hesaplanmıştır. Bulgular ölçeğin tümü için Tablo 5'te sunulmuştur.

Tablo 5. Katılımcıların bilgi güvenliği farkındalığı ölçeğinden elde ettikleri puanların görev yaptıkları birime göre karşılaştırılması

Çalışılan Birim	N	Ort	Ss	Sd	*t*	p
Bilgi Teknolojileri Daire Başkanlığı	72	135,13	22,63	499	8,924	0,000
Diğer Birimler	429	103,29	28,81			

Tablo 5 incelendiğinde, Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin toplamından elde ettikleri puan ortalamalarının 135,13 (ss=22,63) olduğu, diğer birimlerde görev yapan katılımcıların elde ettikleri puan ortalamalarının 103,29 (ss=28,81) olduğu görülmektedir. Puan ortalamalarının karşılaştırılması sonucunda ise, Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcıların ölçeğin toplamından elde ettikleri puanların diğer birimlerde görev yapan katılımcılardan anlamlı olarak daha yüksek olduğu bulunmuştur ($t(499)= 8,924$; $p< ,05$). Bir başka deyişle, Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcılar diğer birimlerde görev yapan katılımcılara oranla daha yüksek bilgi güvenliği farkındalığına sahiptirler.

TARTIŞMA, SONUÇ ve ÖNERİLER

Bilgi ve iletişim teknolojilerinin kullanımı yaşamımızı kolaylaştırmanın yanında pek çok riski ve tehlikeyi de beraberinde getirmiştir. Bu teknolojilerin kötü niyetli ve uygunsuz kullanımının sonucu ortaya çıkabilecek tehditlerin farkında olunmaması ve tehditlerden habersiz olunması nedeniyle bilgi güvenliği riskleri de artmaktadır. Riskleri gidermenin ve kabul edilebilir seviyelere düşürmenin yolu insana yatırım yapmaktan geçmektedir. Yapılan çalışmalar incelendiğinde bilgi güvenliği konusunda bilgi sistemlerinin güvenliğini sağlamaya yönelik olduğu ve kullanıcıların bilinçlendirilmesine yönelik çeşitli tavsiyeler ve alınması gereken tedbirler yer almaktadır.

Bu çalışmada kadın katılımcıların bilgi güvenliği farkındalığı ile erkek katılımcıların bilgi güvenliği farkındalığı benzer seviyede olduğu gözlemlenmiştir. Aynı şekilde Okul, Şimşek, Hafçı ve Barış (2018) konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalığını inceledikleri çalışmasında aynı sonuca ulaşmışlardır. Bu durum Keser, Çetinkaya ve Güldüren (2016)'in ortaöğretim öğrencilerine uyguladığı bilgi güvenliği farkındalığı belirleme çalışmasından farklıdır. Ortaöğretim öğrencileri arasında erkek öğrencilerin bilgi güvenliği farkındalığının kız öğrencilerden daha yüksek olduğu bulunmuştur. Yılmaz, Şahin ve Akbulut (2016)'un öğretmenlerin dijital veri güvenliği farkındalığı üzerine yaptığı çalışmasında ise erkek öğretmenlerin kadın öğretmenlere göre dijital veri güvenliği farkındalığının daha yüksek olduğu bulunmuştur. Arıtürk (2015)'ün mühendislik öğrencileri arasında yapmış olduğu çalışmada kadınların erkeklere göre bilgi güvenliği ve bilgi farkındalığı konusundaki davranışlarının daha yüksek olduğu görülmüştür. Tekerek ve Tekerek (2013)'in ilk ve ortaöğretim öğrencilerinin farkındalıklarını belirlemek üzere yaptığı çalışmada da kız öğrencilerin erkek öğrencilere nazaran daha yüksek farkındalık düzeyine sahip olduğu görülmüştür.

Kamu çalışanlarının bilgi güvenliği farkındalıkları yaş aralıklarına göre incelendiğinde 40 yaş altı gruplarda bilgi güvenliği farkındalık seviyesinin 40 yaş üstü katılımcıların bilgi güvenliği farkındalık ölçeğinden aldıkları toplam puandan yüksek olduğu görülmektedir. Gökmen ve Akgün (2015) çalışmalarında yaşın öğretmen adaylarının bilgi güvenliği bilgilerinde bir farklılığa neden olmadığı sonucuna ulaşmıştır. Aynı şekilde Okul, Şimşek, Hafçı ve Barış (2018) konaklama işletme yöneticilerinde bilgi güvenliği farkındalığı incelediği çalışmasında benzer sonuçlara ulaşmıştır. Ancak Bostan ve Akman (2011) çalışmalarında kadın ve ileri yaştakilerin bilgisayar güvenliği hakkındaki hassasiyetlerinin azaldığını tespit etmişlerdir.

Bilgi güvenliği farkındalığı eğitim düzeyine göre incelendiğinde lise ve altı eğitim seviyesine sahip katılımcıların farkındalık seviyelerinin düşük, üniversite ve üstü eğitime sahip katılımcıların ise yüksek olduğu görülmüştür. Bu sonuç eğitim seviyesi arttıkça bilgi güvenliği farkındalığının arttığını göstermektedir. Oktay ve Çakır (2012) ise öğretmenlerin bilgi güvenliği farkındalığını inceledikleri

çalışmalarında durumu destekleyen sonuçlara ulaşmışlardır. Öğretmenlerin lisans ve yüksek lisans düzeyi ile ön lisans düzeyi arasında anlamlı bir farklılığın olduğu görülmüş olup eğitim seviyesi arttıkça farkındalığın arttığı yönünde sonuca ulaşılmıştır. Tekerek ve Tekerek (2013)' in ilk ve ortaöğretim öğrencilerinin farkındalıklarını belirlemek üzere yaptıkları çalışmada eğitim düzeyi arttıkça farkındalığın arttığı yönünde sonuçlara ulaşılmıştır.

Kamu çalışanlarının çalıştıkları birime göre bilgi güvenliği farkındalıkları karşılaştırıldığında Bilgi Teknolojileri Dairesi Başkanlığı gibi teknik eğitim almış çalışanların olduğu birimin ölçeğin toplam puanından çok yüksek olduğu dolayısıyla birimde çalışanların farkındalıklarının diğer birimlerde çalışanlardan yüksek olduğu görülmüştür. Bu durum Karacı, Akyüz ve Bilgici (2017)' nin yapmış olduğu çalışmada internet ve bilgisayar güvenlik eğitimi alan öğrencilerin bilgi güvenliği tutumlarının daha olumlu olduğu görülmüştür. Bu durum beklenen sonucu desteklemektedir.

Siber güvenlik ve bilgi güvenliği konusunda yaşanan tehditler ve yaşanan kayıplar ileride yaşanabilecek tehdit ve kayıplar konusunda bilgi vermektedir. Bu konuda alınması gereken tedbirlerin çeşitliliği, çokluğu ve ihtiyaç duyulan koordinasyon ve işbirliğini ortaya çıkarmaktadır.

İnternet teknolojisinin baş döndürücü hızla gelişmesine paralel olarak getirdiği tehditler artmakta ve bunlara karşı alınabilecek güvenlik önlemleri ve teknolojileri de gelişerek artmaktadır. Ne var ki, yasal ve idari düzenlemeler bu hızı gerisinde kalmaktadır. Bu nedenle konunun hukuki boyutu gelişmeler dikkate alınarak yeniden düzenlenmelidir.

Mart (2012) çalışmasında bilgi güvenliği okullarda zorunlu bir ders olarak küçük yaşlardan itibaren verilmesi, bilgi iletişim teknolojileri ve internetin kullanımında bilgi güvenliği farkındalığını oluşturulmasına yönelik önerilerde bulunmuştur. Bu önerisi ileriye ışık tutacak şekildedir. Zira okul çağında eğitim gören çocuklar gelecekte bir kurum çalışanı olacaklardır. Gelecekte bireyler hangi konumda ve işle alakadar olursa olsun devletle ve özel sektörle yapacakları işler bilgisayar ortamında internet üzerinden yapılacağı düşünüldüğünde bilgi güvenliği ile ilgili bilincin okul çağında verilmesi hem kişisel verilerin korunmasında hem de kurumsal açıdan personelden kaynaklanan bilgi güvenliği risklerini en aza indirilmesinde etkili olacağı öngörülmektedir.

Bilgi ve iletişim teknolojilerindeki gelişmelerle birlikte artık geleneksel bilgi güvenliği yaklaşımları yerini kurumsal hatta ulusal ve küresel bilgi güvenliği yaklaşımları ve bilgi güvenliği politikalarına bırakmıştır. Ülkemizde ise bilgi güvenliği alanında ve farkındalık konusunda sıkıntılar görülmektedir. Bunun için öncelikle bilgi güvenliğine bakış açılarının değiştirilmesi gerekmektedir. Bilgi güvenliğini sadece bilginin korunması işi olarak düşünmek yerine ülke kalkınmasında gerekli olan kritik altyapılar, e-devlet hizmetleri vb. vatandaşı hizmette yararlanmak için kullandığı her bilgisayar ve cihazın güvenliği olarak düşünmek gerekir.

Şahinaslan ve arkadaşlarına (2009) göre son yıllarda kurumlara yapılan saldırılar artık yıkıcı olmaktan ziyade bilgi sızdırma, bilgi hırsızlığı ve istihbarat amacıyla yapılmaktadır.

Kurumlarda bilginin paylaşıldığı o bilgiye erişmek için yetkisi olan kişilerin yapacakları çok küçük hatalar ve dikkatsizlikler, bilerek ya da bilmeyerek yapılan her türlü ihmal veya suistimal teknik olarak tüm önlemleri boşa çıkaracaktır. Bu nedenle kurumlar, özellikle kamu kurumları kurum faaliyetlerine uygun olan güvenlik politikalarını da kapsayan kurum çalışanlarının niteliklerine göre farkındalık eğitimleri vererek kamu bilgi güvenliği kültürü oluşturma noktasında çalışmalıdır.

Araştırmadaki bulgular ve alanyazın incelemelerinden elde edilen sonuçlar neticesinde bilgi güvenliği farkındalığının bir defaya mahsus oluşturulup bırakılacak bir iş değil sürekli yenilenmek zorunda olan bir süreç olduğu söylenebilir. Bu sebeple yenilikler takip edilerek sürekli ve belirli periyodlarla çalışanlara verilen eğitimlerin yenilenmesi gerekmektedir. Bu şekilde çalışanların konuya verilen önemin farkına varması, görevlerini yerine getirirken yeterli sorumluluğu hissetmesi ve doğabilecek risklerden sorumlu olduğunu bilmesi ile bu farkındalığı sürdürmesi sağlanabilecektir. Ancak eğitim ile bilgilendirmenin tek başına yeterli farkındalığı oluşturmadığı bilimsel çalışmalarda yer almaktadır. Pek çok çalışan yeterli bilgi seviyesine sahip olduğu halde sürekli ekran köşelerinden çıkan bilgilendirme ve uyarılar sebebiyle duyarsızlaştığını aktarmaktadır. Bu sebeple çalışanların dikkatlerini çekecek ve akılda kalacak şekilde bilgilendirmeler yapılırken kendi bilgilerini de sınama imkânı bulabilecekleri güvenlik testleri veya habersiz tatbikat ve sınamalar yapılarak ödüllendirme

yöntemiyle teşvik sağlanmalıdır. Ayrıca çalışanlar aynı zamanda vatandaş konumunda oldukları için Güvenli İnternet Günü gibi belirli tarihlerde kutlanan ve bilgi güvenliği farkındalığını amaçlayan ulusal çalışmaların kapsamının artırılarak etkili olması için gerekli desteğin ilgili kurumlarca verilmesi ve daha geniş bir kesimde ilgi uyandırması sağlanmalıdır.

KAYNAKLAR

Arıtürk, M. (2015). Bilgi farkındalığı ve bilgi güvenliğinin karşılaştırılması. *XVII. Akademik Bilişim Konferansı Bildirileri*, 178-185, Eskişehir.

Baykara, M., Daş, R. ve Karadoğan, İ. (2013). Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. In *1st International Symposium on Digital Forensics and Security (ISDFS'13)* (pp. 231-239).

Bıçakcı, S., Ergun, F. D. ve Çelikpala, M. (2015). Türkiye'de siber güvenlik. *Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kağıtları Serisi*, *1*, 1-35.

Bostan, A. ve Akman, İ. (2011). Kullanıcı açısından bir durum tespiti. *IV. Ağ Ve Bilgi Güvenliği Sempozyumu Bildiriler Kitabı*, s.51-55.

Boyacı, M., Benzer, R. ve Ciylan, B. (2016). Siber güvenlik ve yapay sinir ağları yaklaşımıyla bir değerlendirme. *3. Uluslararası Yönetim Bilişim Sistemleri Konferansı*, 32.

Brakensiek, F. C. (2002). Knowledge Management for EHS Professionals. Occupational *Health-Safety*, 72-74.

Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi güvenliği ve süreçleri üzerine bir inceleme, *Politeknik Dergisi*, *9*(3), 165-174.

Davenport, T. H. ve Prusak, L. (2001). İş dünyasında bilgi yönetimi. (Çev.: Günhan Günay), Rota Yayınları, İstanbul.

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), 1-15.

Erol, O., Şahin, Y. L, Yılmaz, E. ve Haseski, H. İ. (2015) Kişisel siber güvenliği sağlama ölçeği geliştirme çalışması. *International Journal of Human Sciences*, Sakarya.

DIKW Hiyerarşisi ve Dijital Devrim. (2011). 18.12. 2018 tarihinde http://www.ulugsungur.com/2011/11/bilgi-bilgi-hiyerarsisi-ve-dijital.html adresinden erişilmiştir.

Güldüren, C., Çetinkaya, L., & Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *Elementary Education Online*, *15*(2).

Güngör, M. (2015). Ulusal bilgi güvenliği: Strateji ve kurumsal yapılanma. T.C Kalkınma Bakanlığı Uzmanlık Tezi, Ankara.

Gökmen, Ö. F. ve Akgün, Ö.E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi*, *44*(1).

Karacı, A., Akyüz, H. İ. ve Bilgici, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi*, *25*(6).

Karakoç, M. A., (2011). Bilişim suçlarına genel bakış, bilişim suçlarını önleme çalışmaları ve güvenli internet kullanımı. Suç Önleme Sempozyumu Bildiriler Kitabı, s.419-423, Bursa.

Keser, H. ve Güldüren, C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) Geliştirme çalışması, *Kastamonu Üniversitesi Kastamonu Eğitim Dergisi*, *23*(3), 1167-1184.

King, W. R. ve He, J. (2005). Understanding the role and methods of meta-analysis in IS research. *Communications of the Association for Information Systems, 16*, 665-686.

KVKK. (2018). 100 Soruda Kişisel Verilerin Korunması Kanunu. 15.11.2020 tarihinde https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf adresinden erişilmiştir.

Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı*, Yayımlanmamış Yüksek Lisans Tezi, Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Kahramanmaraş.

Oktay, S. ve Çakır, R. (2012). İlköğretim öğretmenlerinin teknoloji kullanımları ve teknolojiye yönelik tutumları arasındaki ilişkinin incelenmesi. X. Ulusal Fen Bilimleri ve Matematik Eğitimi Kongresi, Niğde.

Öğün, M. N. ve Kaya, A. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. *Güvenlik Stratejileri Dergisi*, İstanbul.

Öğütçü, G. (2010). *E-dönüşüm sürecinde kişisel bilişim güvenliği davranışı ve farkındalığın analizi*. Başkent Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.
Solomon, M. ve Chapple, M. (2005). Information security illuminated. Boston: Jones and Bartlett Publishers.
Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri, *Akademik Bilişim, 9,* 11-13.
Şimşek, G., Okul, T., Hafçı, B. ve Barış, Z. (2018) Konaklama işletmesi yöneticilerinde bilgi güvenliği farkındalığı: Kuşadasındaki beş yıldızlı oteller örneği. *Uluslararası 83 Türk Dünyası Turizm Araştırmaları Dergisi*, Kastamonu.
T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi Başkanlığı (2011). Bilgi Toplumu İstatistikleri 2011.
Tekerek, M. ve Tekerek, A. (2013). A research on students' ınformation security awareness. *Turkish Journal of Education, 2*(3), Kahramanmaraş.
Türkiye Cumhuriyeti 5237 sayılı Türk Ceza Kanunu, Kişisel Verileri Koruma Kanunu, 2016.
Ünver, M. ve Canbay, C. (2010). Ulusal ve uluslararası boyutlarıyla siber güvenlik. *Elektrik Mühendisliği Dergisi*, 438, 94-103, Ankara.
Ünver, M., Canbay, C. ve Mirzaoğlu, A. G. (2011). Siber güvenliğin sağlanması: Türkiye'deki mevcut durum ve alınması gereken tedbirler. Uzmanlık Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.
Vural, Y. ve Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. *Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi Dergisi, 23*(2), 507-522.
Yavanoğlu, U., Sağıroğlu, Ş. ve Çolak, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi, 15*(1), 15-27.
Yılmaz, E., Şahin, Y. L. ve Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education*, Sakarya.

Extended Abstract

The purpose of this study is to reveal the information security awareness of public employees. In order to ensure information security, security policies are determined and implemented individually, institutionally and nationally. However, no matter how cautiously and strictly these policies are formed, every system is as strong as its weakest link, and when the human factor is ignored, it causes serious problems for the system. It is important for the user to be aware of the value of the information to be endangered and the risks that may occur depending on which area the system is being used in order to ensure information security. The beginning of the cyber-attacks started with the broadcasting of some unidentified slang messages during the public presentation of the radio receiver, which is said to be safe in England. In the ongoing process, simple attacks such as cross site scripting, distributed denial of service, auto coordinated attack, denial of services and staged attacks, much more complex and comprehensive, much more detailed, much more difficult to understand and precautionary systems have taken tough and costly attacks. While the attack complexity increases, the level of knowledge of the attacker identity decreases and the variety of attacks continues to increase. Attacks use security vulnerabilities in the system in order to penetrate and damage information systems. Just as immunity collapses or breaks open, aggressors such as viruses and bacteria waiting to enter our body damage information systems. The most important factor in causing threats to harm computer systems is technical and individual weaknesses. Weaknesses and weaknesses in security systems can be considered as security vulnerabilities. Threat sources and threat actors who see these vulnerabilities damage the information system. Failure to make software updates or sufficient security configurations, the lack of sufficient technical knowledge of the personnel, and the low level of knowledge and awareness of the personnel against security breaches cause information security violations. In general, there are personal data security measures that the smallest unit, namely the individual, should take to ensure information security. Among these, the passwords used for different purposes (ie internet shopping sites, bank passwords, computer opening passwords, etc.) must be independent from each other, contain different symbols, numbers, characters and at least 8 characters, secret questions and answers used for password reminders are difficult to find. backing up files that are thought to be important on the computer to a secure environment, deleting unsafe and unknown e-mails without opening them, not logging in to unknown web pages in e-mails, leaving the page with the 'Logout'

command in encrypted transactions, not sharing personal information, money, credits, etc. from social networks or via e-mail. ignoring requests etc. such measures are included. It is also important to ensure corporate information security, which directly affects the information security of individuals as well as information security. A wide variety of technologies is used to ensure corporate information security. The main ones of these systems are firewalls, outside-inside attack detection systems and inside-outside attack systems. Authentication and encryption of the data sent are preferred to ensure the integrity and confidentiality of the data transported between networks. Cyber-attacks in recent years have moved from an individual dimension to a cross-country dimension. These attacks mostly target critical structures, and public institutions are among these critical structures. Therefore, the awareness of information security of personnel working in public institutions and organizations is important. This research is a descriptive survey model. In the literature review, scales that were previously carried out for various groups such as teachers, university students, high school students, secondary school students, lecturers and parents were examined. Information Security Awareness Scale developed by Keser and Güldüren (2015) was used as data collection tool. Cronbach's alpha reliability coefficient of the scale is 97. In this study, once again, the Cronbach alpha reliability coefficient was calculated as 97 for the whole scale. The scale consists of thirty-four questions and two sub-dimensions. In the scale, the first sub-dimension is attacks and threats, and the second is the protection of personal data. Data collection was carried out with 501 public employees. Employees were asked to answer scale questions with various information including gender, age range, education level and the unit they work in. At the end of the study, it was seen that public employees had a medium level of information security awareness according to the average score they got from the scale. It has been observed that our participants have a similar level of information security awareness among the male and female participants, and the information security awareness level of the Information Technologies employees who have received technical training and the participants under the age of 40 are high. In addition, it was seen in the study that our participants with a university level education have higher awareness of information security than those with a high school or lower education level. In our study, although the information security level of the participants was at a medium level, they knew that information security is important during face-to-face interviews, but they thought that this was the responsibility of the technical unit, and they thought that they did not need to be aware of this situation. This situation once again shows the importance of information security awareness in establishing a corporate information security culture. For this reason, efforts should be made to increase the information security awareness of public employees throughout the country, because awareness of information security is not a job to be created and left only once, but a process that must be constantly renewed. For this reason, it is necessary to renew the trainings given to the employees continuously and periodically by following the innovations. In this way, it will be ensured that employees become aware of the importance given to the subject, feel sufficient responsibility while performing their duties, and maintain this awareness by knowing that they are responsible for the risks that may arise.