



**KAMU KURUMU VE ÖZEL SEKTÖRE YÖNELİK BİLGİ GÜVENLİĞİ
FARKINDALIĞI ÜZERİNE BİR İNCELEME**

Sena NEZGİTLİ

**YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI**

**GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ**

EYLÜL 2022

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İmza

Sena NEZGİTLİ

27/09/2022

KAMU KURUMU VE ÖZEL SEKTÖRE YÖNELİK BİLGİ GÜVENLİĞİ
FARKINDALIĞI ÜZERİNE BİR İNCELEME
(Yüksek Lisans Tezi)

Sena NEZGİTLİ

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

Eylül 2022

ÖZET

Bu çalışmanın yapılmasındaki temel amaç; gün içerisinde birçok bilgiye ulaşan kamu kurumu ve özel sektör çalışanlarının ulaştıkları bilginin güvenliği konusundaki farkındalık düzeylerini belirleyerek iki sektör çalışanları arasındaki bilgi güvenliği farkındalık düzeylerini kıyaslamaktır. Bilgi güvenliği farkındalığı konusunda, alanyazın başta olmak üzere birçok ulusal ve uluslararası çalışmalar mevcuttur. Alanyazın çalışmaları incelendiğinde kişilerin bilgi güvenliği farkındalık düzeylerinin çalıştıkları sektör farklılığına göre nasıl eğilim gösterdiğine yönelik bir çalışma ile karşılaşılmamıştır. Bu nedenle bu çalışma, özgün niteliktedir. Bu çalışma, tarama modeli kullanılarak Ankara ilinde belirlenen kamu kurumu ve özel sektörde bilgi ve iletişim bölümlerinde çalışan 138 kişi ile gerçekleştirilmiştir. Toplanan verilere, Mann-Whitney U ve Kruskal-Wallis testleri uygulanmıştır. Araştırma bulgularına göre katılımcıların bilgi güvenliği farkındalık düzeylerinde; kurum türü, yaş, cinsiyet, çalışılan pozisyon, öğrenim durumu, işyerlerinde bilgi güvenliği farkındalığı hakkında verilen eğitimlerin/kursların sıklık derecesine göre anlamlı farklılaşma olmadığı görülürken; işyerinin bilgi güvenliği politikasına sahip olması, bu politikayı uygulama derecesi, işyerinde verilen bilgi güvenliği farkındalığı eğitimleri/kursları, bu eğitimlerin/kursların fayda derecesine göre anlamlı farklılaşma görülmüştür. Bu nedenle kişilerin bilgi güvenliği farkındalık düzeyinin artırılması için bilinçlendirme faaliyetlerinin (eğitim, kurs vb.) sektör ayırt etmeksizin işyerleri tarafından yürütülmesi önerilmektedir. Ayrıca çalışanların bilgi güvenliği farkındalık düzeyinin artırılması için işyerlerinin bilgi güvenliği politikasına sahip olması ve bu politikayı istikrarlı bir şekilde uygulaması önerilmektedir.

Bilim Kodu : 92401

Anahtar Kelimeler : Bilgi güvenliği, bilgi güvenliği farkındalığı, kurumsal bilgi güvenliği

Sayfa Adedi : 105

Danışman : Doç. Dr. Şahin GÖKÇEARSLAN

AN INVESTIGATION ON INFORMATION SECURITY AWARENESS FOR THE
PUBLIC AND PRIVATE SECTOR

(M. Sc. Thesis)

Sena NEZGİTLİ

GAZİ UNIVERSITY
INFORMATICS INSTITUTE

September 2022

ABSTRACT

The main purpose of this study is to compare the information security awareness levels between the employees of the two sectors by determining the level of awareness of public institutions and private sector employees who access a lot of information during the day. There are many national and international studies on information security awareness, especially in the literature. When the studies in the literature are examined, no study has been encountered on how the information security awareness levels of people tend to differ according to the sector they work in. Therefore, this study is original. This study was carried out with 138 people working in the information and communication departments of the public institution and private sector determined in the province of Ankara using the scanning model. Mann-Whitney U and Kruskal-Wallis tests were applied to the collected data. According to the research findings, the information security awareness levels of the participants, while it is seen that there is no significant difference according to the frequency of the trainings/courses given on the type of institution, age, gender, position, education level, awareness of information security in the workplaces, a significant differentiation was observed according to the workplace having an information security policy, the degree of implementation of this policy, the information security awareness trainings/courses given in the workplace, and the degree of benefit of these trainings/courses. For this reason, it is recommended that awareness-raising activities (training, courses, etc.) be carried out by workplaces, regardless of sector, in order to increase the level of information security awareness of people. In addition, it is recommended that workplaces have an information security policy and implement this policy consistently in order to increase the level of information security awareness of employees.

Science Code : 92401

Key Words : Information security, information security awareness, corporate information security

Page Number : 105

Supervisor : Assoc. Prof. Dr. Şahin GÖKÇEARSLAN

TEŞEKKÜR

“Kamu Kurumu ve Özel Sektöre Yönelik Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme” isimli bu tezin hazırlanması sürecinde bana hasta yatağında duaları ile destek veren rahmetli babacığım Yavuz NEZGİTLİ’ye sonsuz teşekkür ederim.



İÇİNDEKİLER

	Sayfa
ÖZET	iv
ABSTRACT	v
TEŞEKKÜR	vi
İÇİNDEKİLER	vii
ÇİZELGELERİN LİSTESİ	ix
ŞEKİLLERİN LİSTESİ	x
KISALTMALAR	xi
1. GİRİŞ	1
2. BİLGİ GÜVENLİĞİ, BİLGİ GÜVENLİĞİ KÜLTÜRÜ VE BİLGİ GÜVENLİĞİ FARKINDALIĞI	17
2.1. Bilgi Güvenliği ile ilgili Kavramlar	17
2.1.1. Bilgi kavramı	17
2.1.2. Bilgi güvenliği kavramı ve bilgi güvenliği unsurları	17
2.1.3. Bilgi güvenliğini tehdit eden unsurlar ve bilgi güvenliğini sağlama yöntemleri	26
2.1.4. Bilgi güvenliği farkındalığı kavramı	29
2.1.5. Bilgi güvenliği kültürü ve bilgi güvenliğinde insan faktörü	29
2.1.6. Bilgi güvenliği ile ilgili ulusal ve uluslararası alanda yapılan etkinlikler	31
3. ADLİ BİLİŞİM VE KURUMSAL BİLGİ GÜVENLİĞİ FARKINDALIĞI	35
3.1. Kurumsal Bilgi Güvenliği ve Farkındalığı	35
3.1.1. Kurumsal bilgi güvenliği	35
3.1.2. Kurumsal bilgi güvenliği farkındalığı ve insan faktörü	39

Sayfa

3.1.3. Kurumsal bilgi güvenliği farkındalığı ve kültürü	40
3.2. Kurumsal Bilgi Güvenliği Farkındalığında Adli Bilişimin Rolü	41
3.3. Kurumsal Bilgi Güvenliği Farkındalığı ile İlgili Yapılan Alanyazın Çalışmaları.....	44
4. YÖNTEM.....	49
5. ARAŞTIRMA BULGULARI	55
6. TARTIŞMA VE DEĞERLENDİRME	61
7. SONUÇ VE ÖNERİLER.....	71
KAYNAKLAR	75
EKLER	97
EK-1. Kişisel bilgi formu	98
EK-2. Bilgi güvenliği farkındalığı ölçeği	100
EK-3. Bilgi güvenliği farkındalığı ölçeği kullanım izin belgesi.....	103
EK-4. Etik Kurul Kararı	104
ÖZGEÇMİŞ	105

ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 1.1. Bilgi güvenliği farkındalığı üzerine etki ilişkisi olduğu düşünülen etmenler	14
Çizelge 4.1. Araştırmaya katılan çalışanlar hakkındaki demografik özellikleri.....	50
Çizelge 4.2. Normallığın sınanması.....	53
Çizelge 5.1. Bilgi güvenliği farkındalığının kurum türüne göre Mann Whitney U Testi sonucu	55
Çizelge 5.2. Bilgi güvenliği farkındalığı ölçeği ve ortalaması	55
Çizelge 5.3. Bilgi güvenliği farkındalığının cinsiyete göre Mann Whitney U Testi sonucu	56
Çizelge 5.4. Bilgi güvenliği farkındalığının yaş grubuna göre Kruskal Wallis H Testi sonucu	56
Çizelge 5.5. Bilgi güvenliği farkındalığının öğrenim durumuna göre Kruskal Wallis H Testi sonucu	57
Çizelge 5.6. Bilgi güvenliği farkındalığının çalışanların firmadaki pozisyonuna göre Kruskal Wallis H Testi sonucu	57
Çizelge 5.7. Bilgi güvenliği farkındalığının firmada bilgi güvenliği farkındalığı hakkında eğitim/kurs verilmesine göre Mann Whitney U Testi sonucu	58
Çizelge 5.8. Bilgi güvenliği farkındalığı hakkında eğitim/kurs verilme sıklığına göre dağılımının Kruskal Wallis H Testi sonucu	58
Çizelge 5.9. Bilgi güvenliği farkındalığı hakkında verilen eğitimin/kursun fayda derecesine göre Kruskal Wallis H Testi sonucu	59
Çizelge 5.10. Bilgi güvenliği farkındalığının işyerinde bilgi güvenliği politikasının var olma durumuna göre Mann Whitney U Testi sonucu	59
Çizelge 5.11. Bilgi güvenliği farkındalığının işyerinde bilgi güvenliği politikasının uygulanma derecesine göre Kruskal Wallis H Testi sonucu.....	60
Çizelge 6.1. Kurulan hipotezlerin çalışmalarda kabul edilme/reddedilme durumu	67

ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 2.1. CIA Üçlüsü	19



KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
ABD	Amerika Birleşik Devletleri
AIS	Bilgi Sistemleri Derneği (Association for Information System)
BGYS	Bilgi Güvenliği Yönetim Sistemi
CIA	Gizlilik, Bütünlük, Erişilebilirlik (Confidentiality Integrity Availability)
ENISA	Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency)
FS-ISAC	Finansal Hizmetler Bilgi Paylaşım ve Analiz Merkezi (Financial Services Information Sharing and Analysis Center)
ICIS	Uluslararası Bilişim Sistemleri Konferansı (International Conference on Information Systems)
ISC	Bilgi Güvenliği Konferansı (Information Security Conference)
ISO	Uluslararası Standardizasyon Örgütü (International Organization for Standardization)
ISW	Bilgi Güvenliği Çalıştay (Information Security Workshop)
ITU	Uluslararası Telekomünikasyon Birliği (International Telecommunication Union)
OWASP	Açık Web Uygulama Güvenliği Projesi (Open Web Application Security Project)
TDK	Türk Dil Kurumu
TKDK	Tarım ve Kırsal Kalkınmayı Destekleme Kurumu
UDHB	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
USOM	Ulusal Siber Olaylara Müdahale Merkezi
VNI	Görsel Ağ İndeksi (Visual Networking Index)

1. GİRİŞ

İnsanlık, varoluşuyla beraber dünyayı anlamak için bilgi edinmeye başlamıştır (Çotuksöken, 2018). Edinilen bilgiler sayesinde insanlık dünyayı keşfetme ve onu anlamlandırma gayreti içine girmiştir. Bu gayret sonucunda, keşifler ve bilgi birbirini geliştirerek süreç ilerlemeye devam etmiştir. Bu keşfetme ve bilgi edinme duygusu, insanlığı geliştirme imkânı da sağlamıştır. İnsanlık kendisini geliştirme ve bilgiyi iletme imkânını ilk olarak, çevresi ile iletişim kurarak ve bilgileri sözselsel olarak aktararak sağlamıştır. Ancak sözselsel anlatım her zaman bilgiyi doğru iletme aracı olmamış ve bazı mevcut bilgiler gelecek nesillere aktarılamadan yok olmuştur. Bilginin saklanması ve iletilmesi konusunda yaşadığı zorluklar neticesinde insanlık bilgiyi kalıcı bir kaynak olan yazıya dökmek istemiştir. Bilgi, kimi zaman sembollerle kimi zaman şekillerle kimi zaman da yazı ile çeşitli materyallere aktarılmıştır. Varlığını geliştirerek sürdüren bilgi, yazının bulunması ile kalıcı olarak saklanma ve ihtiyaç duyulduğunda tekrar kullanılabilme imkânı bulmuştur (Özgeldi Büyüktopbaş, 2016). Yazı sayesinde bilgi not edilmiş, saklanmış ve gelecek nesillere aktarılmıştır. Kısacası yazı, bilgi serüveninin ilk değişim ve dönüşüm adımı olmuştur.

Bilgi serüveni, sadece bilginin yazıya aktarılması ile sınırlı kalmamış, insanlığın artan bilgi birikimi sayesinde değişim ve dönüşüm serüvenine devam etmiştir. Bu serüveni, 16. yüzyılda Avrupa'daki bilim Rönesansı'ı (Goody, 2009) ve 18. yüzyılın ikinci yarısında Sanayi Devrimi desteklemiştir (Gürz, 2019). Bu destek neticesinde bilgi; Rönesans ile yeniden yorumlanış ve Sanayi Devrimiyle de insanlık tarafından daha işlevsel bir biçimde kullanılmaya başlanmıştır. Sanayi Devrimi, makinelere komut verme ve bu komutları ona yaptırma gereksinimini ortaya çıkartmıştır. Bu gereksinim sonucunda; Sanayi Devrimi, kendinden bir asır sonra gelecek olan bilgisayarın icadına zemin hazırlamıştır. Bilgisayar icadı ve kullanımı, insanlığın bilgi çağına geçişinde ilk adım olarak görülmüştür (Genç ve Eryaman, 2008). Bu durumda insanlık, bilgi çağına geçiş ile bilgi toplumu olma yolunda ilerlemiştir. Kısacası; bilgi toplumu, insanların birbirleri arasındaki iletişimle başlayan ve teknolojik gelişmelerle ilerleyen bir durumdur (Kocacık, 2003). Bilgi toplumu zemini, 20. yüzyıldan günümüze kadar olan bilgi çağındaki teknolojik gelişmeler ile beslenmiştir (Çalık ve Çınar, 2009). Bilgi toplumunun bir sonucu olarak; bilgi serüvenindeki değişim ve dönüşüm, insanlığın bilgisayar kullanım hızındaki artış ile devam etmiştir. Bilgi, yazıyla çeşitli materyallere aktarıldığı gibi bilgisayar sayesinde de sanal dokümanlara aktarılmıştır.

Bilginin, bilgisayar aracılığıyla sanal dokümanlara aktarılması akıllara, bu bilginin nasıl iletileceği sorununu getirmiştir. Bu sorun, var olan insan iletişimine yeni bir bakış açısı kazandırmıştır. Bunun neticesinde, tıpkı insanlar gibi bilgisayarların da kendi aralarında haberleşme imkânının olma durumu konusunda bir düşünce ortaya çıkmıştır. Bu düşünce sayesinde insanlık; sadece kendi aralarında olan iletişimle sınırlı kalmamış, bilgisayarların da kendi aralarında iletişim kurabileceği ihtimalini düşünmeye başlamıştır. Bilgisayarların birbirleri ile iletişim kurabilme düşüncesi ve bunun uygulanabilirliği konusu 1950’li yıllara dayanmaktadır. Ancak o yıllardaki bilgisayar özellikleri bu durum karşısında yetersiz kalmıştır (İnternet, Koca, 2006). İlerleyen zamanlarda teknolojinin gelişmesiyle belirli uzaklıktaki bilgisayarların bir ağ sistemi vasıtasıyla birbirlerine bilgi iletimi gerçekleşmiştir. Bu ağ, ilk olarak 1969 yılında Amerika Birleşik Devletleri (ABD) Savunma Bakanlığı’nın kurduğu ARPANet olmuştur. ARPANet, insanlık tarihi açısından büyük öneme sahip olan internetin başlangıç aşamasındaki önemli bir gelişmenin ilk adımıdır (Paloque Berges ve Schafer, 2019, s. 1). ARPANet ile internetin temelleri atılmış ancak internetin genele açık hale gelerek kullanılması 1989 yılından sonra olmuştur (Parlak, 2005). Böylece bilgi, bilgisayar ve internetin yaygın kullanımı sayesinde yeni bir değişim ve dönüşüm içine girmiştir. Kısacası, internet sayesinde bilgisayarlar birbirleri arasında iletişim kurmuş (Bayraktar, 2020) ve bilgi paylaşımı gerçekleştirmeye başlamıştır. Bilgisayar ile somut ortamdan soyut ortama aktarılan bilgi, internet sayesinde diğer bilgisayarlara aktarılmış ve tıpkı insanlar arasında olduğu gibi bilgisayarlar arasında da bilgi paylaşımı sağlanmıştır. Sanal ortamda bilgi iletimi için kullanılan en önemli yollardan biri elektronik postalardır. İlk elektronik posta 1971 yılında Tomlinson tarafından kendisine “QWERTYUIOP” mesajını göndermesi ile oluşmuş (Hardy, 1996) ve bu durum insanların sanal ortamda birbirlerine bilgi aktarımı yapmak için yeni bir ufuk açmıştır. Zamanla e-posta; teknolojinin ilerlemesi ve internet kullanım kapasitesinin artması ile beraber metin, resim, ses ve video paylaşımını mümkün kılmıştır. Bilginin, bilgisayar aracılığıyla gerçekten sanala geçişi; internet ve elektronik posta ile de kaynaktan alıcıya sanal olarak aktarımı bilgi için gerçekleşen en büyük değişim ve dönüşümlerden biri haline gelmiştir. Kısacası, internetin kapsam alanının genişlemesi ve internet kullanımının yaygınlaşması, bilgiye ulaşmayı da kolay hale getirmiştir (Ercan, 2009).

Bilgi ve bilgi kaynaklarına internet sayesinde kolay ulaşılması; bilgiye erişim alanını, bölgesel sınırlamalardan kaldırarak küresel bir alana genişletmiştir. Bilginin bulunduğu sanal ortam, ilk kez 1984 yılında Neuromancer romanında *siber uzay* olarak anılmaya

başlanmıştır (Gibson, 1984). Siber uzay hakkında, gerek ulusal gerek uluslararası alanyazında geniş tanımlamalara yer verilmiştir ancak kabul edilen ortak bir tanım mevcut değildir (Polat, 2020). En, boy, yükseklik ve zaman boyutunun var olduğu gerçek dünyanın dışında, beşinci boyut olarak ifade edilen bir yerde siber uzay yer almaktadır (Ünal ve Yarman, 2014, 278). Kısacası siber uzayla kastedilmek istenen, insanın bilgiyi gerçekten sanala taşıdığı beşinci bir boyut olarak düşünülmektedir (Ermiş, 2018). Siber uzay, bilgi paylaşımını ve bilginin hızlı elde edilmesinin yanı sıra çeşitli teknolojilerle (bulut teknoloji gibi) bilginin sanal olarak depolanmasına da imkân sağlamıştır.

Siber uzayın bilgiye sağladığı avantajlar zaman içerisinde değişime uğrayarak kendi ortamında bilginin muhafaza edilmesi konusunda birtakım dezavantajları da beraberinde getirmiştir (Güngör ve Güney, 2017). İnternetin yaygınlaşması ile siber uzaya erişim sağlayan insan ve cihaz sayısında her geçen yıl artış yaşanmaktadır. Çok uluslu ağ şirketi olan Cisco'nun 2009 yılında yayınladığı *Görsel Ağ İndeksi* (GAI-Visual Networking Index) *Raporu*'na göre 2013 yılında internetin 2009 yılına göre neredeyse dört kat daha büyük olacağı belirtilirken (İnternet, Cisco, 2009) yine Cisco 2013 yılında yayınladığı *Görsel Ağ İndeksi* (GAI) *Raporu*'na göre 2017 yılında mobil internet veri kullanımı 2012 yılına göre on üç kat büyüyeceği belirtilmiştir (Cisco, 2013). Yine Cisco 2018-2023 yıllarını kapsayan *Yıllık İnternet Raporu*'nda 2023 yılına kadar dünya nüfusunun yaklaşık 3'te 2'sinin internet erişimine sahip olacağını ve internete bağlı cihaz sayısının da dünya nüfusunun üç katı olacağı öngörülmektedir (Cisco, 2020). Raporlarda da ifade edildiği gibi kısa zaman aralıklarında internet kullanımındaki artışın yanı sıra bağlı cihaz sayısındaki artış da siber uzayın kontrolünü güçleştirmektedir. Bu kontrolsüz artış, siber uzaydaki bilgi güvenliğini tehdit etmekte (Gökçearslan, Nezgıtlı ve Çakır, 2020) ayrıca siber uzayın kontrolünü güçleştiren her unsur, siber uzayda bilgi varlığının yaşam alanını da riske atmaktadır. Siber uzayın kısmen kontrol edilemeyen yapısı büyük zarar veren saldırılara neden olabilmektedir (Bıçakcı, 2014).

Siber uzayda bilginin varlığını sürdürebilmesi ve güvende kalabilmesi için bilginin bu ortamdan gelebilecek tehditlere karşı korunması gerekir. Siber uzayda bilgiyi tehdit eden unsurlar; bilişim tehditleri ve insana bağlı tehditler olarak iki grupta sınıflandırılabilir (Rençber ve Mete, 2017). Bilişim tehditlerine; kötücül yazılım (Kulakoğlu, 2013), sistemde yazılımsal olarak bırakılan açıklıklar örnek olarak verilebilir. İnsana bağlı tehditler; sosyal

mühendislik, kimlik avı, oltalama gibi sistem içinde var olan kullanıcılara yönelik yapılan eylemlerdir. Bu iki tehdit grubu kıyaslandığında insana bağlı tehdit unsurları siber uzaydaki bilgi varlığına daha çok zarar vermektedir. Sonuçta, bilişim sistemindeki açıklar teknolojinin yardımıyla kapatılabilir ancak yanılma potansiyeli yüksek olan insanın bu tehditler karşısında geride bırakılması bilgi güvenliğini riske atacaktır (Çetin, 2014).

Siber uzayda bilginin güvenli bir şekilde varlığını sürdürebilmesi, bu ortamda karşılaştığı tehditlere karşı etkin bir güvenlik politikasının olmasına ve bu politikanın kişilerce uygulanmasına bağlıdır. Bilgiyi güvende tutma ve koruma duygusu, bilginin var olduğu ilk zamanlardan beri gündemdedir (Özdemir, 2019). Ancak bilginin siber uzayda karşılaştığı çalınma, bozulma, değiştirme ve yetkisiz kişilerce ele geçirilme gibi ciddi tehlikeler ile karşı karşıya kalması bilgi güvenliğini daha çok tehdit etmiştir. Siber uzay, hızlı ve kolay bilgiye ulaşma imkânı sunsa da her zaman doğru ve güvenilir bilgiye erişim imkânı sunamayabilir. Bu yüzden, siber uzayda bilgi güvenliği kavramının önemi daha çok artmıştır. Bilgi güvenliği için içerisinde bilginin bulunduğu sistemlerin, bilgi güvenliğinin temel unsurlarının sağlanması gereklidir. (Canbek ve Sağıroğlu, 2006). Bu özelliklerin korunması, bilginin siber uzayda korunmasını sağlayacaktır. Bu ilkelerin korunması ancak sistem açıklarının kapatılması ve bilinçli bireyler tarafından sağlanabilir.

Bilgi güvenliği konusunda uygun davranışları sergilememe potansiyeli yüksek olan insan faktörü, sisteme isteyerek veya istemeyerek geri dönüşü olmayan zararlar verebilir. Güvenliğin en zayıf unsuru olarak görülen *insan* (Gündüz ve Daş, 2016) tarafından yapılan yanlış bir davranış yetkisi olmayan kötü niyetli kişilerin sisteme erişimini sağlayarak bilgi güvenliği için tehdit oluşturabilir. Bilgi güvenliğini tehdit eden siber saldırılar; teknolojik açıkların kapatılması ile insan faktörüne yönelmeye başlamıştır (Ünal ve Ergen, 2018). Örneğin; İran'ın nükleer tesisine yönelik yapılan Stuxnet saldırısında, usb bellekle sisteme bulaşan *solucan*ın sistemi imha etmesi sonucunda ülkenin kritik altyapısına verdiği zarar (Shakarian, Shakarian ve Ruef, 2013), Rusya tarafından Estonya'daki kamu kurumlarını ve özel sektörü hedef alan siber saldırılar sonucunda verilen zararlar (Gürkaynak ve İren, 2011), Gürcistan'ın altyapı sistemlerine yönelik zararlar (Yılmaz, 2017), Türkiye'de hizmet veren bir bankaya uzun süreli ulaşılamamasından kaynaklı ortaya çıkan zararlar (İnternet, Cumhuriyet, 2021), Türkiye'de milli güvenlik açısından oluşturulan erişim engellemesine karşı yapılan engelleme aşma yöntemlerinin bilinçsiz kişilerce kullanımından dolayı siber

ortamda bilgi güvenliğine yönelik yapılan saldırılar (Gök, 2012) durumun ciddiyetini göstermektedir. Dünyadaki gibi Türkiye’de de bilgi güvenliği konusunda bilinçsiz kişiler, sazan avlama saldırılarında siber uzaydaki saldırganların kimlik hırsızlığı ve diğer kötü amaçlı faaliyetlerine maruz kalarak hassas içerikli bilgilerini paylaşmaktadır (Vural ve Sağıroğlu, 2008). Bütün bu örneklerin ortak noktası, yapılan saldırılar karşısında bilinçsiz bireyler, kurumlar ve ülkelerin olmasıdır. Stuxnet saldırısında kaynağı bilinmeyen bir usb belleğin sisteme yerleştirilmesi, Estonya’daki bazı bankaların siber saldırılar karşısında önceden önlem alarak daha az zarar görürken kamu kurumlarının gereken özeni göstermeyerek yapılan saldırıdan büyük hasar alması (Bıçakcı, 2012), Türkiye’de erişim engelini aşmaya çalışan bilinçsiz kişilerin bilgi güvenliğine zarar vermesi maddi ve manevi ciddi tehlikelere neden olmaktadır.

İnsanın bilinçsiz davranışı sonucunda gerçekleşen olaylar sonucunda; bilgi güvenliğinde *insan boyutunun* düşünülmesine ve bilgi güvenliği farkındalığı kavramının gündeme gelmesine neden olmuştur (Yılmaz, Şahin ve Akbulut, 2015). Bilgi ve bilgi kaynaklarına temas eden insanların bilgi güvenliği hakkında farkındalık düzeyleri arttırılmalıdır (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009). Örneğin, Türkiye’nin Ulusal Yargı Ağı Bilişim Sistemi (UYAP) ve içinde barındırdığı bilgilerin çeşitli saldırılara karşı korunması için gerekli önlemlerin alınması (İnternet, HaberlerCom, 2013), *81 İlde, 81 Siber Kahraman* projesi ile farkındalık seminerlerinin yapılması (İnternet, Dijital Dönüşüm Ofisi) bilgi güvenliği için önemli faaliyetlerden bazılarıdır.

İnsanın bilgi güvenliği farkındalık düzeyinin belirlenmesi üzerine çeşitli çalışmalar yapılmıştır. Osterman Research’un 2019 yılı Ekim ayında Amerika’da çeşitli kuruluşlarda tam ve yarı zamanlı çalışan bin on beş kişiye yönelik bilgi güvenliği farkındalık düzeylerini ölçmek üzere yaptığı MediaPRO isimli çalışmada; çalışanların büyük çoğunluğunun işyerlerini siber tehditlere karşı koruyamadığı belirtilmiştir. Yine aynı çalışmada; katılımcıların % 17’si sosyal mühendislik yöntemini bildiğini ve % 27’sinin de bilgisayar platformlarından kötücül yazılım bulaştığını anlayabileceği (İnternet, Osterman Research, 2020) belirtilmiştir. Bu sonuçlara göre; çalışanların bilgi güvenliği hakkında yetersiz kalması, çalıştıkları işyerleri için ciddi birer güvenlik tehdidine dönüşebilir.

Alanyazında kişilerin bilgi güvenliği farkındalık düzeylerinin farklı etmenlere göre ölçümlendiği birçok çalışma yürütülmüştür. Bu çalışmalarda; çeşitli öğrenim durumu, meslek grupları ve sektör çalışanları için bilgi güvenliği farkındalık düzeyi ortaya konmuştur. Öğrenim durumu olarak; ortaöğretim öğrencilerine yönelik (Gökçearsan, Günbatar ve Sarıtepeci, 2021), lise öğrencilerine yönelik (Dönmez, 2019) üniversite öğrencilerine yönelik (Karaoğlu, Yılmaz ve Sezer, 2014; Avcı ve Orçun, 2020; Göldağ, 2021) bilgi güvenliği farkındalık düzeyleri ölçülmüştür. Öğretmenler (Çetinkaya, Güldüren ve Keser, 2017), bilişim çalışanları (Ceylan, 2019), güvenlik güçleri (Taner ve Kılıç, 2019), öğretim elemanları (Güldüren, 2015), otel işletme yöneticileri (Okul, Şimşek, Hafçı ve Barış, 2018), kalite yöneticileri (Çelikçöp ve Yazar, 2019), banka çalışanları (Alemdaroğlu, 2020), kamu çalışanları (Özdemir ve Uluyol, 2021), KOBİ çalışanları (Çatuk, 2018) gibi farklı meslek grubu ve farklı sektörlerde çalışan bireylerin bilgi güvenliği farkındalık düzeylerinin ölçülmesine yönelik çalışmalar yapılmıştır. Bu çalışmaların ortak amacı, seçilen örneklemdaki insan grubunun bilgi güvenliği farkındalık düzeyini belirlemek ve kişilerin bilgi güvenliği farkındalığı hakkında güçlü yönlerle beraber zayıf yönleri de anlamaya yardımcı olacaktır. Belirlenecek bu güçlü ve zayıf yönlerde ilerde oluşturulacak olan bilgi güvenliği farkındalık faaliyetlerine katkı sağlayacaktır. Bu çalışmaların ortak çıkarımı; bilgi güvenliği farkındalığında, teknolojiye yatırım yapmaktan ziyade insana yönelik yapılacak çeşitli eğitim ve uygulama faaliyetleri ile bilgi güvenliği farkındalık düzeyini belirlemektir.

Alanyazın incelendiğinde bilgi güvenliği farkındalığı belirli bir grup, meslek veya sektör ile sınırlandırılmış olup iki farklı sektörün kıyaslanarak bilgi güvenliği farkındalık düzeyini ortaya koyan bilişim çalışanlarını kapsayan bir çalışmayla karşılaşılmamıştır. Bu nedenle bu çalışma, bilgi ve bilgi paylaşımına maruz kalan kamu kurumu ve özel sektör çalışanlarının bilgi güvenliği konusunda farkındalık düzeylerini belirleyerek iki sektör çalışanlarının ellerinde bulunan veya paylaştıkları bilginin güvenliği konusunda farkındalık düzeyini tespit etme imkânı sunmaktadır. Bu çalışmada, kamu kurumu ve özel sektörde çalışan bireylerin bilgi güvenliği konusundaki farkındalıkları incelenmiştir.

Problem durumu / Konunun tanımı

Alanyazında bilgi güvenliği ile ilgili Canbek ve Sağiroğlu (2006) çalışmasında bilginin siber uzaydaki tehditlerine karşı yapılması gereken güvenlik süreçlerini ele alırken, Güngör (2015) de ulusal bilgi güvenliği için gerekli olan kurumsal yapılanma ile stratejiler konusunu

ele almıştır. Alkan, Atalay, Canbek ve Bilirgen (2012) siber güvenlik kültürünün oluşması ve siber güvenlik tehditlerine karşı kritik altyapıların korunması hususunda kurum, kuruluş ve işletmelerle beraber yönetici, çalışan ve kullanıcıya yönelik bilgi güvenliği farkındalığını arttıran etkinlikler düzenlenmesi gerektiğini önermektedir. Erol, Ceyhan ve Sağıroğlu'nun çalışmasında; siber saldırılar karşısında bireysel, kurumsal ve ulusal bilgi güvenliği farkındalığının yaşam döngüsü ortaya konmuştur. Alanyazın dikkate alındığında kamu ve özel sektörde bilişim çalışanlarını kapsayan bilgi güvenliği farkındalığını inceleyen bir çalışmaya rastlanmamıştır. Ancak Özdemir ve Uluyol (2021) cinsiyet, yaş, eğitim durumu, çalışılan birime göre; Öztezcan ve Çetinkaya (2017) cinsiyet ve yaşa göre kişilerin bilgi güvenliği farkındalık düzeyini belirlemek için yaptıkları çalışmalar mevcuttur. SANS Enstitü'nün 2021 Güvenlik Farkındalığı Raporu'na göre; birçok kuruluşun çalışanları için güvenlik bilinci konusuna eğilmedikleri (İnternet, SANS, 2021) ifade edilmiştir. Çalışanların bilgi güvenliği farkındalığı, işyeri için önem arz etmektedir. Lim, Chang, Maynard ve Ahmad'ın (2009) çalışmasında, örgüt kültürünün çalışanlar üzerinde etkisinden bahsetmiştir. Bu çalışma, bilgi güvenliği kültürünün oluşmasında örgüt kültürünün rolünü ifade etmiştir. Johnson ve Goetz'in (2007) çalışmasında, kurumsal bilgi güvenliği sağlaması konusunun işyerindeki herkesin görevi olduğunu belirtilmiş ve örgütsel bir hareket ile yürütülmesi gerektiği ifade edilmiştir. Maynard, Ruighaver ve Chia'nın (2002) çalışmasında, gelişen teknolojinin işyerinin sahip olduğu bilgi varlıklarını riske atarak tehdit edebildiği ifade edilerek bunun sonucunda bilgi güvenliği hassasiyetinin arttırılarak bu konunun örgüt kültürünün bir parçası olan tüm çalışanlarca benimsenmesi gerektiği ifade edilmiştir. Bu çalışmalar, örgüt kültürü ile kurumsal bilgi güvenliğinin birbirlerine katkı sağladığını ve birbirleriyle bağlantılı olduğunu ifade etmektedir. Örgüt kültüründe örgütsel davranış içinde yer alan; iş etiği (Yavan, 2016), yönetim (Koç, 2014), iş davranışı (Çalışkan, 2014), örgütsel adalet algısı (Kılıçaslan, 2010), iş doyumu (Acar, 2019) gibi konuları mevcuttur. Kamu kurumu ve özel sektör çalışanlarının, alanyazında yapılan çalışmalarda bu konularla ilgili farklı davranış gösterme eğilimleri bulunmuştur. Yapılan bir çalışmada, *iş etiği olarak rakibin unutarak gittiği dokümanı alma* konusunda kamu çalışanlarının %41'i ikilemde kalırken, özel sektör çalışanlarının %60'ı dokümanı almayacaklarını belirtmişlerdir (Özkaya ve Şengül, 2006). Bu durum, kamu ve özel sektör çalışanlarının iş etiği konusunda farklı tutum sergilediklerini gösterirken bir başka çalışma da ise kamu ve özel sektör yöneticilerinin yönetsel narsizim düzeyinin farklılığından bahsedilmiştir (Önder, 2014). Gökçen ve Çetin (2022)'in çalışmasında, özel sektör çalışanlarının iş davranışı ve performansı kamu çalışanlarına göre daha yüksektir. Yavuz'un (2010) çalışmasında, özel

sektör çalışanlarının örgütsel adalet algısı kamu kurumu çalışanlarına göre daha yüksek çıkarken Fidan'nın (2011) çalışmasında, özel sektör yöneticilerinin zamanını yönetmedeki duyarlılıkları kamudaki yöneticilere göre daha fazla olduğu belirtilmiştir. Eğinli'nin (2009) çalışmasında, kamu çalışanlarının iş doyumu özel sektör çalışanlarına göre yüksek çıkmıştır. Örgüt kültürünün bir parçası olan iş etiği, yönetim, iş davranışı, örgütsel adalet algısı ve iş doyumu gibi konularda kamu kurumu ve özel sektör çalışanlarının farklı tutum sergilediği görülmektedir. Örgüt kültürü ve bilgi güvenliği arasındaki bağlantı düşünüldüğünde örgüt kültürünün bünyesinde bulunan iş etiği, iş davranışı ve benzeri konularda farklı tutum sergileyen kamu ve özel sektör çalışanları bilgi güvenliğinin parçası olan bilgi güvenliği farkındalığı konusunda da farklı tutum ve davranış sergileme durumlarını akıllara getirerek bu iki sektör çalışanlarının bilgi güvenliği farkındalık düzeylerinin belirlenmesi için bu iki grup seçilmiştir.

Hipotezlerin oluşturulması

Alanyazında kurum türü ile kişilerin bilgi güvenliği farkındalığı ilişkisinin incelendiği bir çalışma ile karşılaşılmamıştır. Ancak kamu kurumu ve özel sektör çalışanlarının bilgi güvenliği farkındalık düzeylerinin ölçüldüğü bazı çalışmalar mevcuttur. Özdemir ve Uluyol'un (2021) çalışmasında, kamu çalışanlarının orta seviye bilgi güvenliği farkındalığına sahip olduğu belirtilmiştir. Taner'in (2019) çalışmasında emniyet çalışanlarının bilgi güvenliği farkındalık düzeyinin düşük olduğu belirtilmiştir. Okul, Şimşek, Hafçı ve Barış'ın (2018) çalışmasında, konak işletme yöneticilerinin bilgi güvenliği farkındalığının yüksek olduğu belirtilmiştir. Parsons, McCormac, Pattinson, Butavicius ve Jerram'ın (2014) çalışmasında, Avustralya'daki kamu kurumu çalışanlarının bilgi güvenliği hakkındaki bilgi birikiminin teorik olarak yüksek olsa bile bunun bilgi güvenliği farkındalığına yansımadağı ve kişilerin bilgi güvenliği farkındalığının yeterli seviyede olmadığı ifade edilmiştir. Bu nedenle, bu çalışmalardan çıkan sonuçlar doğrultusunda H1 kurulmuştur.

H1: Özel sektör çalışanlarının bilgi güvenliği farkındalığı kamu kurumu çalışanlarına göre daha yüksektir. (Ana hipotez)

Farklı meslek grubu çalışanlarının bilgi güvenliği farkındalık düzeyinin ölçüldüğü alanyazın çalışmaları, bilişim çalışanlarının diğer meslek grubu çalışanlara göre daha yüksek bilgi güvenliği farkındalığına sahip oldukları gözlemlenmiştir. Mart'ın (2012) çalışmasında,

mühendislerin bilgi güvenliği farkındalığı diğer meslek grubu çalışanlarına göre daha yüksek çıkmıştır. Başka bir çalışmada, okullarda öğrencileri teknoloji ile buluşturan ve öğretmenlere teknolojik materyaller ile ders yürütme imkânı sunan FATİH projesi kapsamında çalışan öğretmenlerin, bilgi güvenliği farkındalığı diğer öğretmenlere göre daha yüksek çıkmıştır (Keser ve Yayla, 2021). Avcı ve Oruç'un (2020) çalışmasında; mühendislik fakültesi öğrencilerinin bilgi güvenliği farkındalığı, eğitim fakültesi öğrencilerine göre daha yüksek çıkmıştır. Teker'in (2019) ve Yayla'nın (2018) çalışmasında; Bilgi Teknolojileri öğretmenlerinin bilgi güvenliği farkındalığı, diğer branş öğretmenlerine göre daha yüksek çıkmıştır. Alemdaroğlu'nun (2020) çalışmasında, bilgi teknoloji müdürlüğünde çalışanların bilgi güvenliği farkındalığı diğer müdürlüklerde çalışan kişilere göre daha yüksek çıkmıştır. Bu çalışmalardan çıkan sonuçlar doğrultusunda H2 kurulmuştur.

H2: Bilişim çalışanlarının bilgi güvenliği farkındalığı diğer çalışanlara göre daha yüksektir.

Kişilerin cinsiyet farklılığının bilgi güvenliği farkındalığı üzerinde etkili olduğuna yönelik yapılan çalışmalar ile karşılaşılmıştır Dönmez'in (2019), Talan ve Aktürk'ün (2021), Göldağ'ın (2021), Teker'in (2019) çalışmasında, erkek öğrencilerin bilgi güvenliği farkındalığı kız öğrencilere göre daha yüksek çıkmıştır. Çelikçöp ve Yazar'ın (2019), Yılmaz, Şahin ve Akbulut'un (2016), Solmaz'ın (2020), Keser ve Yayla'ın (2021), Alemdaroğlu'un (2020), Öztezcan ve Çetinkaya'nın (2017) çalışmasında da erkek katılımcıların bilgi güvenliği farkındalığı kadınlara göre daha yüksek çıkmıştır. Gündüzalp'in (2021) çalışmasında erkeklerin kişisel siber güvenlik farkındalığı kadınlara göre daha yüksek çıkmıştır. Bu çalışmalardan çıkan sonuçlar doğrultusunda H3 kurulmuştur.

H3: Erkek çalışanların bilgi güvenliği farkındalığı kadın çalışanlara göre daha yüksektir.

Kişilerin yaş farklılığının bilgi güvenliği farkındalığı üzerinde etkili olmadığına yönelik yapılan çalışmalar ile karşılaşılmıştır. Okul ve diğerlerinin (2018) çalışmasında otel işletme yöneticilerinin yaş düzeyi kişilerin bilgi güvenliği farkındalığı üzerinde bir etki oluşturmamıştır. Ayrıca Çelikçöp ve Yazar'ın (2019), Alemdaroğlu'nun (2020), Teker'in (2019), Öztürk ve Çakır'ın (2022) çalışmalarında da kişilerin yaşı bilgi güvenliği farkındalığı üzerinde anlamlı fark oluşturmamıştır. Bu çalışmalardan çıkan sonuçlar doğrultusunda H4 kurulmuştur.

H4: Katılımcıların yaş düzeyi bilgi güvenliği farkındalığı üzerinde etkili değildir.

Kişilerin öğrenim durumu, bilgi güvenliği farkındalığı üzerinde etkili olmadığına yönelik yapılan çalışmalar ile karşılaşılmıştır. Mart'ın (2012) çalışmasında çalışanların doktora, lisansüstü, lisans veya ön lisans mezunu olmaları bilgi güvenliği farkındalığında bir değişikliğe neden olmazken Okul ve diğerlerinin (2018) çalışmasında da benzer sonuçlar ortaya çıkmıştır. Alemdaroğlu'nun (2020), Baran ve Şener'in (2020) yürüttüğü çalışmalarda da öğrenim durumu bilgi güvenliği farkındalığı üzerinde etkili bir faktör olmamıştır. Bu çalışmalardan çıkan sonuçlar doğrultusunda H5 kurulmuştur.

H5: Katılımcıların öğrenim durumu bilgi güvenliği farkındalığı üzerinde etkili değildir

Çalışanların işyerindeki pozisyonunun bilgi güvenliği farkındalığı üzerinde etkili olmadığına yönelik yapılan çalışmalar ile karşılaşılmıştır. Özaslan'ın (2019), Kurt'un (2019), Okul ve diğerlerinin (2018) çalışmasında kişilerin işyerinde çalıştıkları pozisyon farklılıkları bilgi güvenliği farkındalığı üzerinde anlamlı farka neden olmamıştır. Bu çalışmalardan çıkan sonuçlar doğrultusunda H6 kurulmuştur.

H6: Katılımcıların işyerinde çalıştıkları pozisyon bilgi güvenliği farkındalığı üzerinde etkili değildir.

Çalışanların bilgi güvenliği farkındalığı hakkında eğitim almaları, kişilerin bilgi güvenliği farkındalığı üzerinde olumlu yönde etkili olduğunu gösteren çalışmalar ile karşılaşılmıştır. Fakeh, Zulhemay, Shahibi ve Zaini (2012) çalışmasında, çalışanlara bilgi güvenliği eğitimlerinin verilmesinin bilgi güvenliği farkındalığını arttırdığı sonucu elde edilmiştir. Shehri ve Clarke'n (2007) yaptığı çalışmada; bilgi güvenliği konusunda eğitim almayan çalışanların bilgi güvenliği farkındalığı eğitim alanlara göre daha düşük çıkmıştır. Keser ve Yayla'nın (2021) çalışmasında, daha önce bilgi güvenliği farkındalığı eğitimi alan öğretmenlerin, eğitim almayanlara göre daha yüksek bilgi güvenliği farkındalığına sahip olduğu belirtilmiştir. Akyol ve Uzun'un (2021) çalışmasında; Sağlık Meslek Yüksekokulu öğrencilerinden oluşan çalışma grubunda, daha önce bilişim dersini alan öğrencilerin almayanlara göre daha yüksek farkındalığa sahip olduğu belirtilmiştir. Bilen'in (2016) çalışmasında, aynı işyerinde farklı branşlarda çalışan kişilerde bilgi güvenliği eğitimi alanların almayanlara göre bilgi güvenliği farkındalığının daha yüksek olduğu belirtilmiştir. Ayrıca Gündüzalp'in (2021) çalışmasında, yürütülen bilgi güvenliği farkındalık eğitimlerinin kişilerin bilgi güvenliği farkındalık düzeyini yükselttiği belirtilmiştir. Haeussinger ve Kranz'ın (2013) çalışmasında, bilgi güvenliği programlarının özel sektör

çalışanlarının bilgi güvenliği farkındalığına ve bilgi güvenliği davranışına katkı sağladığı belirtilmiştir. Hagen ve Albrechtsen'in (2009) çalışmasında; bilgi güvenliği e-öğrenme programlarının, çalışanların bilgi güvenliği farkındalığına katkı sağladığı ifade edilmiştir. Bu çalışmalardan çıkan sonuçlar doğrultusunda H7 kurulmuştur.

H7: Katılımcıların işyerinde aldıkları bilgi güvenliği farkındalık eğitimi/kursu bilgi güvenliği farkındalığı üzerinde etkilidir.

Çalışanların aldıkları bilgi güvenliği farkındalık eğitim/kurs faaliyetlerinin verilmesindeki sıklık derecesinin, kişilerin bilgi güvenliği farkındalığı üzerinde etkili olmadığına yönelik yapılan çalışmalar mevcuttur. Pattinson, Butavicans, Parsons, McCormac ve Calic'in (2017) yaptığı çalışmada, kişilere verilen bilgi güvenliği eğitimlerinin verilme sıklığı bilgi güvenliği farkındalığı için belirleyici bir etken olmamıştır. Farooq'un (2013) çalışmasında; katılımcılara, *bilgi güvenliği farkındalık eğitimini ne sıklıkla almak istediklerinin* sorulduğu soruya verilen cevaplarda ilk sırayı *talep üzerine* seçeneği alırken ikinci sırayı *yılda bir* eğitim alınması gerektiği seçeneği yer almıştır. Ayrıca bu çalışma için katılımcılar arasından bu soruya cevaplayan sadece % 1'i bu eğitimi *sıklıkla* almak istediği belirtilmiştir. Kısaca, kişiler bilgi güvenliği eğitimini ihtiyaç duyulduğunda ya da yılda bir almak istemektedir. Pattinson, Butavicius, Lillie, Ciccarello, Parsons, Calic ve McCormac'ın (2019) çalışmasında, bireylerin aldığı bilgi güvenliği eğitiminin bilgi güvenliği farkındalığı üzerine etkiliyken eğitimin alınma sıklığının kişilerin bilgi güvenliği farkındalığı üzerine bir etkisinin bulunmadığı ifade edilmiştir. Bu çalışmalardan çıkan sonuçlar doğrultusunda H8 kurulmuştur.

H8: Katılımcıların işyerinde aldıkları bilgi güvenliği farkındalık eğitimin/kursun verilmesindeki sıklık derecesi kişilerin bilgi güvenliği farkındalığı üzerinde etkili değildir.

Bilgi güvenliği farkındalık eğitiminin kişilerce fayda derecesi ve bu eğitimlerin bilgi güvenliği davranışını oluşturmada etkin rol oynadığına yönelik yapılan çalışmalar mevcuttur. Stephanou'n (2008) çalışmasında, bilgi güvenliği farkındalık eğitiminin kişinin doğru bilgi güvenliği davranışı sergilemesine olumlu katkı sağladığı belirtilmiştir. Gökçearslan, Günbatar ve Sarıtepeci'nin (2021) çalışmasında, ortaokul öğrencileri için bilişim teknolojileri dersinden alınan faydanın bilgi güvenliği farkındalığını da etkilediği belirtilmiştir. Yayla'nın (2018) çalışmasında; öğretmenler aldıkları bilgi güvenliği farkındalığı eğitimleri hakkındaki görüşlerinde, konu hakkında farkındalık düzeyini

yükselttiği ve eğitimleri yararlı buldukları ifade edilmiştir. Tschakert ve Ngamsuriyaroj'ın (2019) çalışmasında, *kimlik avı* konulu eğitimin, eğitimi alan kişilerce faydalı bulunduğu belirtilmiştir. Bauer, Bernroider ve Chudzikowski'n (2017) çalışmasında, bilgi güvenliği yöneticilerinin bilgi güvenliği farkındalık programlarını yararlı buldukları belirtilmiştir. Bu çalışmalardan çıkan sonuçlar doğrultusunda H9 kurulmuştur.

H9: Katılımcıların işyerinde aldıkları bilgi güvenliği farkındalık eğitiminin/kursunun fayda derecesi kişilerin bilgi güvenliği farkındalığı üzerinde etkilidir.

Bilgi güvenliği farkındalığı ile işyerinin bilgi güvenliği politikasına sahip olması arasındaki ilişkinin incelendiği çalışmalar mevcuttur. Yıldırım'ın (2006) çalışmasında bankaların yarısından fazlasının (3/2) bilgi güvenliği politikasına sahip olduğu ve bu politikanın bankadaki iç denetim ile risk yönetimine katkıda bulunduğu ifade edilmiştir. Ayrıca bu çalışmada, işyerinde bilgi güvenliği politikası olmasının bilgi güvenliği farkındalığı üzerinde etkili olduğu ifade edilmiştir. Meral ve Bülbül'ün (2021) çalışmasında, bilgi güvenliği politikasının işyerlerinde kurumsal bilgi güvenliğinin sağlanmasına yardımcı olduğu belirtilmiştir. Bulgurcu, Çavuşoğlu ve Benbasat'ın (2009) çalışmasında, bilgi güvenliği farkındalığının bilgi güvenliği politikasına katkı sağladığı ifade edilmiştir. Haeussinger ve Kranz'ın (2013) çalışmasında, bilgi güvenliği farkındalığı ile bilgi güvenliği politikası arasındaki uyum etkisi incelenmiş ve bu iki unsurun birbirlerini geliştirdiği vurgulanmıştır. Chan ve Mubarek'ın (2012) çalışmasında, yönetsel olarak bilgi güvenliği farkındalığı eksikliğinin, bilgi güvenliği politikasını olumsuz etkilediği belirtilmiştir. Bu çalışmalardan çıkan sonuçlar doğrultusunda H10 kurulmuştur.

H10: İşyerinin bilgi güvenliği politikasına sahip olması kişilerin bilgi güvenliği farkındalığı üzerinde etkilidir.

Bilgi güvenliği farkındalığı ile işyerinde bulunan bilgi güvenliği politikasının uygulanma derecesi arasındaki ilişkinin incelendiği çalışmalar mevcuttur. Gebru (2020), Etiyopya'daki özel banka çalışanlarının bilgi güvenliği farkındalığını etkileyen etmenler üzerine bir çalışma yürütmüştür. Çıkan sonuçlarda, banka çalışanlarının bilgi güvenliği farkındalık düzeyleri düşük çıkmıştır. Bunun nedeni; işyerinde bilgi güvenliği politikasının yeterince uygulanmamasıdır. Gebru (2020) çalışmasında, kişilerin bilgi güvenliği farkındalığının artırılması için kurumsal bilgi güvenliği politikasının yönetsel olarak uygulanması ve çalışanlara uygulatılması gerektiği hakkında öneride bulunmuştur. Bulgurcu, Çavuşoğlu ve

Benbasat'ın (2010) çalışmasında, çalışanların bilgi güvenliği farkındalığının işyerindeki bilgi güvenliği politikasına uyum gösterme konusunda etkili olduğu ifade edilmiştir. Bu çalışmadan çıkan sonuçlar doğrultusunda H11 kurulmuştur.

H11: İşyerinin sahip olduğu bilgi güvenliği politikasının uygulanma derecesi kişilerin bilgi güvenliği farkındalığı üzerinde etkilidir.

Araştırmanın amacı

Kamu kurumu ve özel sektör çalışanlarının bilgi güvenliği farkındalık düzeylerinin karşılaştırılması bu çalışmanın temel amacıdır. Bu temel amacın yanı sıra çalışanların bilgi güvenliği farkındalığının; yaş, cinsiyet, öğrenim durumu, çalışılan pozisyon, bilgi güvenliği farkındalığı hakkında eğitim/kurs verilme durumu, bilgi güvenliği farkındalığı üzerine eğitim/kurs verilme sıklığı, alınan bu eğitim/kursun fayda derecesi çalışılan işyerinde bilgi güvenliği politikasının mevcut olma durumu ve bu politikanın uygulama derecesi gibi değişkenlere göre farklılaşma durumu incelenmiştir.

Araştırmanın önemi

Gelişen dünyada bilgi edinme, bilgiyi iletme ve depolama konusunda kaynakların siber uzaya yönelmesine neden olmuştur. Bu geçiş, insanlara birçok kolaylık getirse de bilgi güvenliğinde problemlere yol açmıştır. Bu nedenle bilginin siber uzayda güvende kalması ve bilgi güvenliği farkındalığı hakkında siber uzaya nüfuz eden insanların konu hakkında bilinçli olması önemli hale gelmiştir. Kişilerin farkındalık düzeyinin belirlenmesi işyerinde çalışan bireylerin bilgi güvenliği konusunda bilinç düzeyini ortaya koyarak kurum için belirlenecek bilgi güvenliği politikasına katkı sağlanacağı düşünülmektedir. Bu nedenle kamu kurumu ve özel sektör çalışanlarının bilgi güvenliği hakkındaki farkındalık düzeyinin belirlenmesi önemlidir. Bu çalışma, iki sektörde çalışan bireylerin bilgi güvenliği farkındalığını ölçerek kurumların, çalışanları için yürüttükleri bilgi güvenliği farkındalık faaliyetlerinde eksik olduğu konuları görebilme imkânı sunmaktadır. Bu imkân ile belirlenecek kurumsal bilgi güvenliği politikası şekillendirilip işyerlerine etkin bilgi güvenliği politikası hazırlama konusunda yardımcı olacaktır. Ayrıca bu çalışma, sadece sektör farklılığının bilgi güvenliği farkındalığı üzerinde olan etkisini incelemekle kalmamış; ayrıca, cinsiyet, yaş, çalışılan pozisyon vb. birçok farklı etmen ile bilgi güvenliği farkındalığı ilişkisini de kurmaktadır. Çizelge 1.1'de yapılan alanyazın çalışmalarında bilgi güvenliği farkındalığı üzerine etki ilişkisi olduğu düşünülen etmenlerin sıralaması mevcuttur.

Çizelge 1.1. Bilgi güvenliği farkındalığı üzerine etki ilişkisi olduğu düşünülen etmenler

Yapılan Alanyazın Çalışmaları	Kişilerin BGF üzerinde etki ilişkisi olduğu düşünülen etmenler
Yıldırım (2006)	İşyerinin bilgi güvenliği politikasına sahip olma durumu
Stephanou (2008)	Bilgi güvenliği farkındalığı eğitim, bilgi güvenliği davranışı
Bulgurcu ve diğerleri (2009)	Bilgi güvenliği politikası ile uyum
Bulgurcu ve diğerleri (2010)	Bilgi güvenliği politikası gereksinimleri
Mart (2012)	Cinsiyet, yaş, meslek, eğitim durumu bilgisayar ve internet kullanım süresi
Shehri ve Clarke	Güvenlik eğitimi alma durumu
Haeussinger ve Kranz (2013)	Bilgi güvenliği politikası
Farooq (2013)	Bilgi güvenliği farkındalığı eğitim verilme sıklığı
Parsons ve diğerleri (2014)	Kamu çalışanları
Bilen (2016)	Cinsiyet, yaş, eğitim durumu ve işyerinde çalışılan birim
Öztezcan ve Çetinkaya (2017)	Cinsiyet, yaş
Pattinson ve diğerleri (2017)	Bilgi güvenliği farkındalığı eğitim verilme sıklığı
Okul ve diğerlerinin (2018)	Cinsiyet, yaş, pozisyon, mesleki deneyim, öğrenim durumu günlük bilgisayar ve internet kullanım süresi bilgisayar, akıllı telefon ve tablete sahip olmaları
Yayla (2018)	Bilgi güvenliği farkındalık eğitimi fayda derecesi
Ceylan 2019	Cinsiyet, yaş, eğitim düzeyi, bilişim sektöründe çalışma süresi
Çelikçöp ve Yazar (2019)	Cinsiyet, meslek grubu
Dönmez (2019)	Cinsiyet, internet kullanımı, sosyal medya kullanımı
Fakeh ve diğerleri (2012)	Kütüphane farklılığı
Pattinson ve diğerleri (2019)	Bilgi güvenliği farkındalığı eğitimi bilgi güvenliği farkındalığı eğitim alma sıklığı
Taner (2019)	yaş, cinsiyet, meslek medeni durum, eğitim düzeyi çalışılan birim, ünvan, çalışma süresi
Teker (2019)	Cinsiyet, yaş, çalışılan branş
Tschakert ve Ngamsuriyaroj (2019)	Kimlik avı eğitimi
Kurt (2019)	Cinsiyet, yaş, pozisyon, eğitim durumu
Alemdaroğlu (2020)	Cinsiyet, yaş, öğrenim durumu, görev türü, çalışılan birim görev süresi, internet kullanım süresi
Avcı ve Oruç (2020)	Okunulan bölüm farklılığı, sahip olunan sosyal medya hesap sayısı kişisel siber güvenlik davranışı
Gebri (2020)	İşyerinin bilgi güvenliği politikasına sahip olma durumu, işyerinde bilgi güvenliği politikasının uygulanma derecesi
Göldağ (2021)	Cinsiyet, öğrenim durumu, bilgisayar kullanım süresi
Gündüzalp (2021)	Yaş, mesleki deneyim, öğrenim durumu, görev türü

Çizelge 1.1.(devamı) Bilgi güvenliği farkındalığı üzerine etki ilişkisi olduğu düşünülen etmenler

Keser ve Yayla (2021)	Cinsiyet, yaş, bilgi güvenliği farkındalığı eğitim alma durumu görev yapılan okul türü
Özdemir ve Uluyol (2021)	Cinsiyet, yaş, eğitim durumu, çalışılan birim
Talan ve Aktürk (2021)	Öğrencilerin yaşadıkları şehir, cinsiyet, sınıf düzeyi internet ve sosyal medya kullanım süreleri

Çizelge 1.1'e göre yapılan çalışmalarda kişilerin bilgi güvenliği farkındalığı üzerinde etkili olan etmenler arasında en çok cinsiyet, yaş ve öğrenim durumu gibi etmenlerin yer aldığı görülmektedir. Bilgi güvenliği farkındalığı ile bilgi güvenliği politikası arasındaki ilişkinin incelendiği çalışma sayısı daha azdır. Ayrıca yapılan bu çalışmalarda bilgi güvenliği farkındalığı ve cinsiyet, yaş, eğitim durumu gibi etmenler ile sınırlı tutulmuştur. Bu çalışma, alanyazına kişilerin bilgi güvenliği farkındalığı üzerinde etkili olan demografik özelliklere ek olarak bilgi güvenliği farkındalığı eğitimi, alınan eğitimin sıklık ve fayda derecesinin yanı sıra işyerinde bilgi güvenliği politikasının bulunması ve bu politikanın uygulanma derecesi arasındaki ilişkiyi kapsamlı olarak analiz etme imkânı sunmaktadır. Bu nedenle, bu çalışma kensidinden önce yürütülen alanyazın çalışmalarına göre daha kapsamlı ve özgün bir niteliktedir. Sonuçta, daha önce kurum türünün bilgi güvenliği farkındalığı üzerine olan etkisinin incelendiği bir çalışma yürütülmemiştir.

Sınırlılıklar

Yürütülen bu araştırmanın bazı sınırlılıkları mevcuttur. Çalışma esnasında tüm katılımcı bireyler kendi rızaları ile bu çalışmada yer aldıklarından dolayı konu hakkında tercihlerde yanlılığa neden oluşturmuş olabilir. Araştırma Ankara ilinde çalışan 138 kişiden oluşan kamu kurum ve özel sektör bilişim çalışanı ile sınırlandırılmıştır.

Tanımlar

Siber Uzay, insanlığa sanal ve gerçeklik arasında kapı açan beşinci boyutu ifade eder (Ünal ve Yarman, 2014, s. 278).

Kötücül Yazılım (Virüs, Solucan), bir cihaz veya sisteme yetki izni olmadan erişerek bilgiye, bilgi güvenliğine zarar vermek için oluşturulmuş kod parçalarıdır (Utku ve Doğru, 2017, s. 1016). Virüs ve solucan kötücül yazılım türlerindendir.

Casus Yazılım, sisteme gizlice sızıp bilgi toplayan virüs gibi ağı kirleten türlerden biridir (Jian-chuan, Guo-xiang, Xin, 2009, s. 1).

Kimlik Avı/Sazan Avlama, ortalama olarak da bilinir. Kişiyi hassas içerikteki bilgilerini paylaşması için saldırganın kendisini uzman kişi olarak göstererek erişim yetkisi olmadığı bilgilere ulaşmak için kullandığı yöntemlerdir (Jagatic, Johnson, Jakobsson ve Mencher, 2007, s. 94)

Arka Kapı, sistem açıklarını kullanarak sisteme yasa dışı girmek için kullanılan kötücül yazılımdan biridir (Arslan, 2016, s. 6).

Klavye Dinleme, tuş kaydedici olarak da bilinir. Bilgisayar klavyesine veya tuş takımına sahip olan cihazlarda basılan her tuşu kaydederek bunu saldırgana gönderen kötü amaçlı yazılım türüdür (Say ve Sağıroğlu, 2004, s. 3).

Sosyal Mühendislik, güvenliğin en zayıf halkası olan insanı hedef alarak yetkili kullanıcıyı sistemde devre dışı bırakmayı amaçlayan tüm kötü amaçlı faaliyetlerdir (Nezgitli, 2021, s. 37)

Güvenlik Duvarı, sistemde tanımlı kullanıcılara yetki ölçüsünde erişim imkânı sunan güvenlik aracıdır (Karaarslan, 2003, s. 1)

Bulut teknolojisi, zaman ve mekândan bağımsız olarak tüm cihazlardan veri paylaşımı imkânı veren bulut bilişim olarak da bilinen internet veri tabanını kullanan depolama hizmetidir (İnternet, Hosting, 2021).

Bu çalışmanın geri kalanı, Bölüm 2’de; bilgi güvenliğini oluşturan kavramlar, bilgi güvenliği unsurları, bilgi güvenliğini tehdit eden unsurlar, bilgi güvenliği kültür ile beraber insan faktörü, bilgi güvenliği hakkında yapılan ulusal ve uluslararası çalışmalar, kurumsal bilgi güvenliği farkındalığı ile insan faktörü ve kurumsal bilgi güvenliği farkındalığı ile ilgili yapılan alanyazın çalışmalarının neler olduğunu hakkında bilgi verirken; Bölüm 3’de; adli bilişim ve kurumsal bilgi güvenliği farkındalığı ilişkisi sağlanarak adli bilişimin kurumsal bilgi güvenliği farkındalığı için öneminden bahsedilmiştir. Bölüm 4’te: “kamu kurumu ve özel sektör yönelik bilgi güvenliği ölçek” çalışmasının yöntemi, araştırma modeli, çalışma grubu, veri toplama süreci, veri toplama aracına yer verilmiştir. Bölüm 5’te ise, veri analizi sonucu ortaya çıkan araştırma bulguları ifade edilerek Giriş bölümünde kurulan hipotezler ret veya kabul edilmiştir. Bölüm 6’da, bu konu hakkında yapılan alanyazın çalışmaları ile yapılan bu çalışmanın benzerlik ve farklılıkları tartışılırken son bölüm olan Bölüm 7’de ise çalışma için sonuçlar ortaya konarak önerilerde bulunulmuştur.

2. BİLGİ GÜVENLİĞİ, BİLGİ GÜVENLİĞİ KÜLTÜRÜ VE BİLGİ GÜVENLİĞİ FARKINDALIĞI

Bilgi ile beraber gelişen bilgi güvenliği, birçok kavram ve unsuru içinde barındırmaktadır. Bu bölümde bilgi güvenliğinin kapsadığı unsurlar, bilgi güvenliği hakkında yapılan ulusal ve uluslararası çalışmalar ile bilgi güvenliği farkındalığı hakkındaki konular incelenmiştir.

2.1. Bilgi Güvenliği ile İlgili Kavramlar

Bu kısımda, konunun daha rahat anlaşılması için; bilgi, bilgi güvenliği, bilgi güvenliği unsurları, bilgi güvenliğini tehdit eden unsurlar, bilgi güvenliğini sağlama yöntemleri ve bilgi güvenliği farkındalığı konuları açıklanmıştır.

2.1.1. Bilgi kavramı

Bilgi güvenliği kavramının temelini oluşturan bilgi sözcüğü, insanın idrak edebildiği olgu, gerçek ve ilkelerin tümü şeklinde ifade edilir (Türk Dil Kurumu (TDK), 2005, s. 267). Bilgi kavramı, insanın süregelen karar verme davranışında yol gösterici olmuştur (Gülseçen, 2014). Siber uzaya var olan bilgi; bu ortamda oluşturulmuş veri kümesinin organize edilerek işlenmesi sonucu elde edilmesi olarak karşımıza çıkmaktadır (İnternet, Berksoy, 2019). Yukarıda ifade edilen tanımlara ek olarak bilgi, insanın varoluşunu açıklayan, insana yeni değerler katarak gelişmesini sağlayan verilerin bütünüdür. Kısacası bilgi, oluşturulan verinin yapılandırılarak anlamlı hale getirilmesi ile oluşan kavramdır (Güngör, 2015, s. 6).

2.1.2. Bilgi güvenliği kavramı ve bilgi güvenliği unsurları

Bilgi güvenliği, kapsadığı unsurlar bakımından geniş tanım yelpazesine sahip bir kavram olarak karşımıza çıkmaktadır. Bilgi, insanlığın varoluşundan beri süre gelen bir olgudur. Bilgi güvenliğinin sağlanması sorunu da, bilginin üretilmeye başlandığı ilk zamanlardan beri mevcut bir sorundur. Kısacası, bilgi güvenliği de tıpkı bilgi gibi insanlığın var oluşu ile süre gelen bir olgudur. Ancak bilginin bulunduğu ortamların zamanla farklılaşması bilgi güvenliğini sağlama yöntemlerini de değiştirmiştir. Bilgi güvenliği, teknoloji ile yeni bir boyut kazanmıştır. Sistemlerde konumlanan bilgi için güvenliğin nasıl sağlanacağı

konusunda alınması gereken önlemler günümüzde bilgi güvenliğinin temelini oluşturmaktadır (Koçak ve Memiş, 2018). Bilgi güvenliğinin sağlanması için bu kavramın neyi ifade ettiğini anlamak ve bu kavramın kapsam alanını bilmek önemli olacaktır.

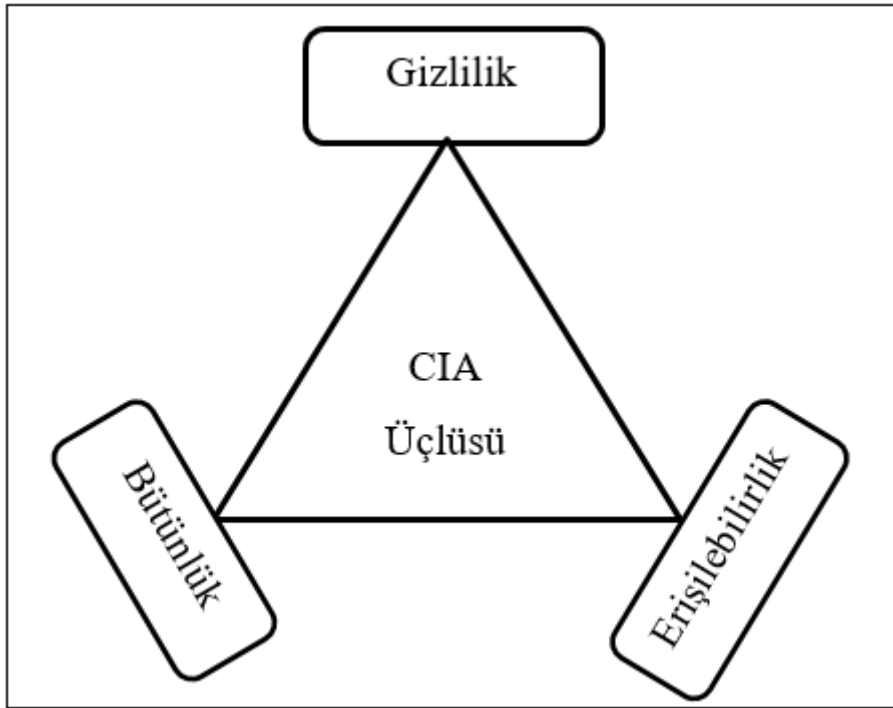
Bilgi güvenliğinin kapsam alanı konusunda birçok ulusal ve uluslararası kurum ve kuruluşların tanımı mevcuttur. Alanyazında, bilgi güvenliği; bilginin var olduğu ortam içerisinde gönderilen hedeften ulaşacağı kaynağa gidene kadar gizlilik, bütünlük ve erişilebilirliğinde bir kayıp olmadan iletilmesi olarak tanımlanmıştır (Vural ve Sağıroğlu, 2008, s. 508). Bir başka tanımda ise bilgi güvenliği; bilginin izinsiz erişimi, kullanımı, üçüncü kişilere aktarımı, ortadan kaldırılması, değiştirilmesi veya bozulmasının önüne geçilmesi olarak ifade edilmiştir (Baykara, Daş ve Karadoğan, 2013, s. 231). Bu durum, bilginin korunması ile beraber bilginin bütünlüğünün muhafaza edilmesi için alınan önlemleri de kapsamaktadır. Kısaca bilgi güvenliği, sahip olunan sistem ve verilerin üçüncü kişiler tarafından zarara uğramasına engel olma isteğidir (Andress, 2014, s. 32). Bilgi güvenliği, aslında kurum ve kuruluşların sahip olduğu bilgi teknoloji sistemlerinin devamlılığının sağlanması ile önem kazanmıştır (Blakley, McDermott ve Geer, 2001).

Kurumsal olarak bilgi güvenliği; izinsiz veya yetkisiz biçimde bilginin kullanımı, değiştirilmesi, açıklanması, yok edilmesi, başkaları ile paylaşılması ve bilgiye zarar verilmesi durumlarına engel olunması isteği şeklinde ifade edilebilir (İnternet, Tarım ve Kırsal Kalkınmayı Destekleme Kurumu (TKDK), 2021). Uluslararası Standartlar Teşkilatı'na (IST) göre bilgi güvenliği; bilgi erişimine yetki verilen kişilerce bilgi üzerinde yapılacak işlemlerde gizlilik, bütünlük, reddedilemezlik, hesap verilebilirlik ve güvenilirlik gibi temel ilkelerin sağlanmasıdır (İnternet, ISO, 2013). Cisco'ya göre bilgi güvenliği; işyeri için önem arz eden bilgilerin değiştirilmesi, bozulması ve yok edilmesi gibi zararlı süreçlerden korumayı amaçlayan işlemlerdir (İnternet, Cisco). Tüm tanımlamalardan yola çıkılırsa bilgi güvenliği, bilginin varoluşu ile kaynağa gidene kadar tam ve eksiksiz bir biçimde iletilmesine ek olarak bilgi teknolojilerinin kapsam alanına giren bir güvenlik durumudur.

Bilgi güvenliği unsurları

CIA modeli olarak bilinen bilgi güvenliğinin temel unsurları, İngilizce “confidentiality (gizlilik), integrity (bütünlük), availability (erişilebilirlik)” kelimelerinin baş harflerinden meydana gelmektedir (Nezgitli, 2021, s. 51). Bilgi için bu üç unsur sağlandığında bilgi

güvenliği de sağlanmış olur. Bu unsurlar, McCumber (1991)'in bilgi güvenliği modelinde “bilginin karakteristiği” kısmında yer alan ve günümüzde güncelliğini koruyan unsurlardır. CIA modeli, alanyazında CIA üçlüsü olarak da karşımıza çıkmaktadır (Samonas, ve Coss, 2014). Bu üçlü, Solomon ve Chapper (2005) tarafından CIA üçgeni olarak da adlandırılmaktadır. Bu temel ilkelere, ITU’nun siber güvenlik tanımında da yer verilmiştir (İnternet, ITU, 2018). Şekil 2.1’de bilgi güvenliğinin temel unsurları olan; gizlilik, bütünlük ve erişilebilirlik unsurları verilmiştir.



Şekil 2.1. CIA üçlüsü (Samonas ve Coss, 2014)

Gizlilik

Bu üç unsurdan ilk unsur olan gizlilik için alanyazında birçok tanımlama mevcuttur. Gizlilik unsuru, var olan veriye/bilgiye erişim yetkisi bulunan kişiler dışında erişimin engellemesini kapsar (Chang ve Lin, 2007, s. 12). Bu unsur, hassas verileri yetkisiz kişilere karşı korumayı hedefler (Taherdoost, Chaeikar, Jafari ve Shojae Chaei Kar, 2013, s. 15). Kapsamlı olarak bakıldığında ise gizlilik unsuru; izni ve yetkisi olmayan kişi veya kişilerin veriye ulaşımına engellemekle beraber sistem içindeki yetkili kullanıcının veri trafiğine hâkim olmasını sağlamayı amaçlar (Bartos, 2016, s. 32).

Gizlilik unsurunun birçok tanımı mevcuttur. Ulusal Siber Olaylara Müdahale Merkezi (USOM); bilişim sistemi ve onu oluşturan verilerin her birine yalnızca yetkisi bulunan kişi

ve sistemlerin erişim sağlaması bununla beraber sisteme ait olan gizli verilerin yetkisi olmayan kişi veya sistemlere aktarılmaması olarak tanımlamaktadır (USOM, 2014, s. 6). Türkiye'nin siber güvenlik konusunda yol haritasını belirleyen 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde ise gizlilik unsuru; bilginin yetkisiz olan her türlü kişi, süreç ve varlıklar açısından kullanılmaması ve açıklanmaması biçiminde tanımlanmıştır (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB), 2016, s. 7).

Bilginin gizlilik ilkesine uyarken bilgiye yetkili kişilerce erişilememesi problemlere yol açacaktır (Alagöz ve Allahverdi, 2011). Gizlilik ilkesi için kurumun bilgi kaynaklarının bulunduğu sistemlerin erişilen bilgi için hassasiyet derecesinin belirlenmesi önem arz etmektedir. Kurumsal yapılanmada, hangi bilgilerin hassas içeriğe sahip olduğu ve bu bilgilere özel erişim izninin gerekip gerekmediği konusunun kurumun bilgi güvenliği politikasında belirlenmesi, gizlilik ilkesinin korunmasını sağlar. Bilgi kaynağına ne oranda erişilebileceğinin belirlenmesi de gizlilik ilkesinin korunmasını sağlayacak diğer bir unsurdur. Gizliliğin belirlenmesi için gizlilik etiketi veya gizlilik kategorisi oluşturulabilir (Cervantes ve Fenz, 2014). Gizlilik etiketi, kurumun sahip olduğu bilgi varlıklarına göre kurumun belirleyeceği kategoriler çerçevesindeki içerik hassasiyetini belirtmek için kullanılır (Oudkerk, Bryant, Eggen ve Haakseth, 2010). Bu nedenle kurumsal bilgi güvenliği için gizlilik ilkesinin sağlanması hem mevcut bilgi varlıklarının gizlilik hususundaki derecelendirilmesine hem de bu derecelendirmenin doğru yapılması için bir etiket sisteminin belirlenmesine ihtiyaç duymaktadır (Henkoğlu ve Yılmaz, 2013).

Bütünlük

Bilgi güvenliğinin diğer bir unsuru da bütünlüktür. Bütünlük unsuru, bilgi üzerinde oluşabilecek tüm zararlı faaliyetlere karşı oluşabilecek tehditler hususunda bilginin korunmasını temsil eder (Baykara ve diğerleri, 2013, s. 239). Bu unsur, oluşturulmuş bilginin hedeften çıkarak ulaşacağı kaynağa varana kadar herhangi bir değişim ve dönüşüm içinde bulunmadan kendini muhafaza etme durumudur (Ada, 2018, s. 11). Bu durum, bilginin bütünlüğüne karşı yetkisiz kişilerce değişiklik yapılmaması anlamını taşır (Henkoğlu ve Yılmaz, 2013, s. 455). Bu sayede bilginin işlenmemiş hali olan verinin yetkisiz kişilerce değiştirilmesinin önüne geçerek veri içeriğine zarar verebilecek tüm işlemler (değiştirme, bozma, silme vb.) için önlem alınmasının hedefler (Can ve Akbaş, 2014, s. 18). Bütünlük unsurunun gerçekleşmesi bilginin gittiği hedefte kendisini de doğrulamış olduğunun bir göstergesidir (Gencer, 2015).

Bilgi güvenliğinde bütünlük ilkesinin kapsamı zaman içerisinde bilgi güvenliği hakkında inkâr edilemezlik unsurunun da ele alınması gerektiğini ortaya koymuştur. Bilginin bütünlüğünde olan değişiklik faaliyetlerinin algılanması, ancak alıcının kaynaktan bilgiyi aldığı ve kaynağın da bilgiyi gönderdiğini kabul etmesi veya durumu inkâr edememesi ile sağlanabilir. Bilgi bütünlüğünün korunması için yapılacak en önemli eylemler; bilgiye erişim sahiplerinin sistemde yaptıkları işlemleri izlemek amacıyla sanal kayıt (log) defterlerinin tutulması, sayısal damgalama ve verilerin şifrelenmesiyle mümkündür. Bu kayıt, bilgi varlıklarının bulunduğu sistemlerdeki kullanıcıların sistemde bulundukları süre içerisinde hangi işlemleri yaptığını göstermektedir (Baykara, Daş ve Gürkan, 2016, s. 292). Bu kayıt, bilginin bütünlüğünü bozacak herhangi bir işlem karşısında, bu işlemin kim tarafından ve ne zaman yapıldığı konusunda bilgi sahibi olunmasını sağlayacaktır. Veri şifrelenmesi ise işlenen verinin bilgi haline dönüştürülmesi ile bilginin sistemler arası iletiminde şifrelenerek kaynaktan alıcıya gidene kadar korunmasını sağlamayı hedefler. Kurumsal yapılanmada bilgi güvenliği, bünyesinde oluşturulan veri kümelerinin gizlilik derecesine göre hangi verilerin şifrelenmesi gerektiği konusunda bir ilke tanımlar (Al-Sanabani, 2016). Bu tanımla sayesinde hem kurum için gizlilik derecesine göre bilgiler sınıflandırılır hem de hassas içeriğe sahip bilgiler şifrelenerek güvenli bilgi iletimi sağlanmış olacaktır. Sayısal damgalama, bilgi bütünlüğünün korunması için görülmeyen (görüntü, video vb.) veya duyulmayan (ses gibi) gizli bir işaretin, sayısal çoklu ortamdaki veriye eklenerek bu verinin damgalanması işlemidir (Kazan ve Vural, 2016, s. 1). Bu sayede verinin oluşmasından yok olma sürecine kadar maruz kaldığı tüm işlemler bu damga aracılığıyla gözlemlenebilir. Tüm bu eylemler, verinin bütünlüğünün korunması için kurumsal politika kapsamında yer alması gereken eylemlerdir (Gülmüş, 2010).

Erişilebilirlik / Kullanılabilirlik

Bilgi güvenliği için üçüncü temel unsur olan erişilebilirlik tıpkı bütünlük unsuru gibi alanyazında farklı kelimelerle karşımıza çıkmaktadır. Erişilebilirlik veya kullanılabilirlik unsuru temelde aynı şeyi ifade etmektedir. Erişilebilirlik unsuru, kişiye izin ve yetki verildiği takdirde bilgiye eksiksiz ve bütün halde ulaşmasının sağlanmasıdır (Karadağ, 2019, s. 34). Bu unsur, erişim yetkisi verilen kişilerin istediği zaman bilgiye ulaşması durumunu ifade eder (Alagöz ve Allahverdi, 2011, s. 50). Erişilebilirlik, yetkili kişiye bilgiyi kullanma koşulu sağladığı için bilgi güvenliğinde önemli bir unsurdur. Kısacası bu unsur sayesinde bilgiye erişim yetkisi bulunan kişiler, bilgiyi her an kullanabilir (Doğantimur, 2009, s. 7).

Bu üç temel unsur bağlamında; bilgi güvenliği için gizlilik, bütünlük ve erişilebilirlik unsurları sistem işleyişini engelleyecek şekilde olmamalıdır. Bilgiye ulaşma konusunda yetki verilmiş kurum çalışanlarının istenen işlem doğrultusunda bilgiyi iletmeleri, dönüştürmeleri ve hatta silmeleri bütünlük unsuruna aykırılık göstermeden bilgiye erişim yetkilerinin var olduğunun bir kanıtıdır. Burada engel olunması gereken durum, bilgiye erişim yetkisi bulunmayan kötü niyetli insanların sisteme yasa dışı bir biçimde sızma girişimleridir. Bu durumda erişim yetkisi ihlal edilmiş olur. Kimlik avı, arka kapı, klavye dinleme, sazan avlama gibi birçok yöntemle yetkili kullanıcıların bilgileri ele geçirilerek sisteme yetkisiz kişilerin girişiyle erişilebilirlik unsurunun yapısı bozulmuş olur. Bu saldırganlara karşı yetki dâhilindeki kurum çalışanları için farkındalık alışkanlıkları geliştirilmeli ve hassas içeriklerin koruma yöntemleri hakkında çalışanlar bilinçlendirilmelidir (Vural ve Sağıroğlu, 2008).

Zaman içerisinde alanyazında bilgi güvenliğine ilişkin tanımlayıcı başka unsurlar ve modeller, McCumber (1991) modeline ve modelindeki üç temel unsura ek olarak dâhil olmuştur. Canbek ve Sağıroğlu (2006); gizlilik, bütünlük, kullanılabilirliğin yanı sıra kimlik doğrulama ve inkâr edememe unsurlarını bilgi güvenliğinin temel unsurları olarak kabul ederken; sorumluluk (izlenebilirlik), erişim denetimi (erişilebilirlik), güvenilirlik ve emniyet gibi unsurları da bu temel unsurların yardımcıları olarak ifade etmişlerdir. Röhrig (2003) ise güvenlik modeli gereksinimlerinde; gizlilik, bütünlük, erişilebilirlik ve hesap verme unsurlarını ele almıştır. Cherdantseva ve Hilton (2013) CIA modelindeki unsurların yeterli olmadığını düşünerek geliştirdikleri güvenlik modelinde bu unsurlara ek olarak; hesap verilebilirlik, güvenilirlik, denetlenebilirlik, inkâr edememe ve mahremiyet unsurlarını da eklemişlerdir. Uluslararası Telekomünikasyon Birliği'nin (ITU) *Gelişmekte Olan Ülkeler için Siber Güvenlik Rehberi'nde (Cyber Security Guide For Developing Countries)* gizlilik, bütünlük ve erişilebilirliğe ek olarak kimlik doğrulama, inkâr edilemezlik ve atfedilebilirlik unsurlarını da temel güvenlik unsurları arasına dâhil edilmiştir (ITU, 2007). Alanyazını ve uluslararası yayınlar dikkate alındığında bilgi güvenliğinin temel unsurlarının tamamlayıcısı olan diğer unsurlar aşağıda açıklanmıştır.

Hesap Verilebilirlik

Hesap vermek; yapılan hareketin/sözün nedenini izah etmek veya yapılan işin sorumluluğunu alma olarak ifade edilmektedir (TDK, 2005, s. 880). Bu tanımdan yola çıkarak hesap verilebilirlik unsuru, bilgi sistemlerine erişim yetkisi olan kişilerin sistemde

yaptıkları işlemlerin sorumluluklarını alarak gerektiğinde kişilere bu işlemleri açıklama yükümlülüğü getirir. Hesap verilebilirlik unsurunun etkin çalışması için sisteme erişim yetkisi olan kişilerin sistem içerisindeki davranışlarının izlenebilmesi ve bunların kayıt altına alınması son derece önemlidir. Bu nedenle bilgi sistemlerine kimin, ne zaman, nerede ve hangi işlemi yapmak üzere sisteme eriştiğinin bilinmesi için sisteme giriş-çıkış kaydının tutulması önemlidir. Hesap verilebilirlik unsuru sayesinde bilginin bütünlüğü de koruma altına alınmış olur. Bu unsur, bütünlük ilkesinin tamamlayıcısı durumundadır (Kurnaz ve Dindaroğlu, 2016).

Bilgi güvenliğinde hesap verilebilirlik unsuru, alanyazında karşımıza bilgi güvenliği sorumluluğu (Al-Rashdi, 2018) ve izlenebilirlik unsuru (Türkiye Bilişim Derneği, 2006) olarak çıkmaktadır. Kurumsal bilgi sistemine karşı geliştirilen davranışlarda, personelin bilgiyi yönetme kabiliyeti ve gerektiği zamanda bilgi üzerinde yapılacak işlemler konusunda hesap verilebileceği bir düzenek oluşturulması önemlidir (Zhu, Zou, Liu ve Gao, 2020). Hesap verilebilirlik unsuru sayesinde insan, siber uzayda yaptığı eylem sonuçlarını üstlenerek bilgi güvenliği hakkındaki etkinliği de arttırılmış olunur (Mellor ve Noyes, 2007). Sonuçta, bilgi güvenliği için hesap verilebilirlik unsuru, kişinin siber uzayda yaptığı işlemler sonucu dijital ayak izini bıraktığı tüm işlemler konusunda sorumlu olduğunu bilerek hareket etmesini sağlar.

Kimlik doğrulama

Çalışılan kurumda yetki verilmiş kişilerin sisteme erişimini mümkün kılmak için kimlik doğrulamasının yapılması oldukça önemlidir. Kimlik doğrulama ile kurum sistemlerine yetkili kişilerin erişimini ve kurum içi personelin yetki derecesine göre sistemlere hangi yetki derecesinden erişebileceği belirlenmiş olur. Kısacası kimlik doğrulama sisteme erişim sağlayan kişinin kim olduğunu ayırt ederek erişim yetkisi verebilir veya erişim yetkisini sonlandırabilir (Uğur ve Soğukpınar, 2014).

Kimlik doğrulama, alanyazında karşımıza kimlik sınanması (Parlakkılıç ve Uysal) olarak da çıkabilmektedir. Bilgi ve bilgi sistemlerinin korunması için kimlik doğrulaması için yaygın olarak şifre yöntemi kullanılmaktadır (Kaya, 2017). Şifre yöntemi, bilgi tabanlıdır. Buna ek olarak, sembol/jeton tabanlı (akıllı kart) ve biyometrik (parmak izi tanıma, yüz tanıma, ses tanıma) tabanlı kimlik doğrulama yöntemleri de mevcuttur (Khan, Aalsalem ve Xiang, 2011). Bu yöntemlerden herhangi biri tercih edilirken kurumun sahip olduğu sistem veya

sistemlerdeki bilginin önem derecesine göre bir ya da birden fazla yöntem kimlik doğrulama için tercih edilebilir.

Güvenilirlik

Güvenilirlik unsuru, sahip olunan bilgi ve bilgi sistemlerinde yapılan faaliyetlerde aksaklık olmadan devam edebilme durumudur. Bilginin kesintisiz bir şekilde var olması ve sistemlerin bilgi teminini güvenli bir şekilde sağlaması gerekir. Güvenilirlik unsuru, bilgiye sahip olan sistem ve sistem kümelerinde istenen sonucun alınmasını sağlamakla birlikte alınan bu sonuç ile sistemden beklenen sonucun kendi içerisinde tutarlılık göstermesine ihtiyaç duyar (Marcinkowski ve Stanton, 2003, s. 2528). Bu unsurun yerine getirilmesi ile kurumsal sistemdeki üretilen, aktarılan ve depolanan bilginin sistemdeki iç tutarlılığı sağlanmış olur ve bu bilgi güvenilirlik özelliği kazanır. Güvenilirlik unsuru, temel olan üç unsurun da yardımcısı konumundadır. Sistemlerin sürekliliği ve doğru çalışmasını sağlayarak diğer unsurlara katkıda bulunur.

Emniyet

Bilgi güvenliğinin ana unsurlarından olan gizlilik unsuruna yardımcı olan unsurlardan birisi de emniyet unsurudur. Bu unsurun amacı da tıpkı güvenlik unsurunun amacında olduğu gibi sistemdeki bilgi ve bilgi kaynaklarının güvenliğini korumaktır. Emniyet unsuru, bilgisayar sistem veya yazılımın kendi işleminde olduğu zaman bulunduğu ortam için oluşan ya da olması muhtemel tüm tehlikeleri önlemek üzere alınan önlemleri kapsar (Canbek ve Sağıroğlu, 2006). Emniyet ve güvenlik unsuru sistemin can simidi gibi davranır ve gizlilik unsurunun en temel yardımcısıdır.

Mahremiyet

Mahremiyet kelimesi, Arapça *mahrem* sözcüğünün kökünden gelerek (Diler, 2014, s. 72) *bir şeyin gizli kalması* anlamına gelmektedir. Mahremiyet unsuru ise kurum ve kurumda çalışanlar için bilgi gizliliğinin korunması için önemli bir unsurdur. Kişisel ve kurumsal mahremiyet konusunda, kurumun sahip olduğu bilgiler hakkındaki yürütülen birçok çalışma için gizlilik ilkesi esas alınarak hareket edilmeli ve bilgiler korunmalıdır. Mahremiyet unsurunun sağlanması için bilgiyi barındıran sistemler için güvenlik unsuru işlevsel hale getirilmelidir (Yüksel, 2005). Sistemdeki bilgiler yetki dâhilinde ifşa edilmelidir. Kurumsal mahremiyet, sadece kurumun sahip olduğu bilgileri değil bunun yanı sıra kurum

çalışanlarının sahip olduğu bilgilerin de gizlilik ilkesini temel alınarak korunmasını gerektirir. Kısacası kurumsal mahremiyet unsuru, gizlilik unsurunun tamamlayıcısı konumundadır. Bilginin gizliliği olmadan mahremiyetinden de söz edilemez (Şahinaslan ve diğerleri, 2009).

Denetlenebilirlik

Denetlenebilirlik unsuru, sistemde bulunan bilgi ve bilgi kaynakları için bir kontrol mekanizması sağlamaktadır. Sistemin çalışma prensibi üretilen bilgi için geriye dönük olarak kontrol edilebilecek şeffaflıkta olmalıdır. Denetlenebilirlik unsurunun tam olarak gerçekleştirilebilmesi için kurumun sahip olduğu sistemler, en üst düzey yetkiye sahip sistem çalışanları tarafından kontrol edilmelidir. Bu kontrol edilme süreci, sistemde bulunan bilgi varlığının kurum içindeki önem derecesine göre farklılık gösterebilir (Konacaklı, 2019).

Denetlenebilirlik unsuru alanyazında erişim denetim (Savolainen, Niemela ve Savola, 2007) olarak da karşımıza çıkmaktadır. Kısaca denetlenebilirlik veya erişim denetimi unsuru, bilgi sistemi veya sistemlerindeki yapılan her bir işlem için önemli bir ihtiyaç (Polic, 2012) olmakla beraber üretilen bilginin gizliliğine zarar gelmesi durumunda kontrolün sağlanmasına yardımcı olur.

İnkâr edememe

Alanyazında inkâr edememe veya inkâr edilemezlik olarak karşımıza çıkan bu unsur, sistemde eylemi gerçekleştiren üçüncü kişinin yaptığı eylemi reddetmesine karşın eylemi kendinin yaptığına dair kanıt gösterme imkânını sağlar (Yan, Qian, Sharif ve Tipper, 2012, 1002). İnkâr edilemezlik ile ilgili protokoller bilginin barındığı sayısal ortamlarda sıklıkla kullanılmaktadır (Kavurucu ve Sever, 2016). Bu unsurun temel amacı, kişinin sistemde yaptığı eylemi inkâr edememesini sağlamaktır (Arda, 2020). İnkâr edememe unsuru kişiye yaptığı işlem için sorumluluk vermektedir. Kısaca inkâr edilemezlik, kişinin sistem içerisinde yaptığı eylem veya eylemleri kanıtlayıp kişiye yaptıklarını reddetme hakkının tanınmamasıdır (Yılmaz ve Salcan, 2008, s. 86). Bu unsur, sayesinde bilgi ve bilgi bütünlüğüne yapılan her türlü tehdit karşısında sisteme girme yetkisi bulunan kişilerin yaptıkları eylemler doğrultusunda sorumluluk almaları sağlanmış olunur. Bu durumda olası bir bilgi güvenliği saldırısında gerçek sorumlunun belirlenmesinde için önem taşımaktadır.

2.1.3. Bilgi güvenliğini tehdit eden unsurlar ve bilgi güvenliğini sağlama yöntemleri

Bilginin yetkisiz ve izinsiz kişilerce erişimi, değiştirilmesi, bozulması, imha edilmesi ve hatta üçüncü kişilere aktarılması (Çam, Aslay ve Özen, 2019, s. 1) bilgi güvenliğini tehdidi anlamına gelmektedir. Bu koşullardan biri veya birden fazlasının gerçekleşmesini neden olan unsurlar ise bilgi güvenliğini tehdit eden unsurlardır. Bilgi güvenliğini siber uzayda tehdit edilmesi ile ortaya çıkan unsurların anlaşılması oldukça önemlidir. Bilgi güvenliğini nelerin riske attığının bilinmesi, belirlenecek bilgi güvenliği modelleri ve stratejilerine karşı önemli bir rehber oluşturacaktır (Tekerek, 2008).

Bilginin siber uzaya aktarıldığı her alanda bilgi güvenliğini tehdit eden durumlar ile karşılaşılabilir. Bu tehdit unsurları bazen kurum dışından olabileceği gibi bazen de kurum içinde çalışan birinin bilerek veya bilmeyerek dikkat etmediği hususlarda da meydana gelebilir. Bilgi güvenliğini tehdit eden unsurların kapsamı, teknolojinin ilerlemesi ile siber uzaya dâhil olan ekipmanlarla genişlemektedir. Kurum dışından gelişen tehdide, bir işletmenin muhasebe faaliyetleri yürütülürken işletme dışından bilgi hacklenmesi veya işletmenin rakipleri tarafından işletmenin bilgi sistemine verilen zararlar (Demir, 2005, s. 150) örnek gösterilirken; işletme içinde gelişen tehdide, görev tanımının belirsiz olmasından kaynaklı olarak bu kayıtların tüm çalışanlara açılması örnek gösterilebilir. Başka bir örnek vermek gerekirse; teknolojinin ilerlemesi ve her sektöre nüfuz etmesi sonucu özellikle kütüphane gibi bilgi edinme merkezlerinde son zamanlarda sadece yazılı kaynaklara değil, aynı zamanda siber uzaydaki belgelerden bilgi edinmek isteyen insanlar için internet erişimi mevcut hale (İnternet, Milli Kütüphane, 2021) gelmesi ve bu mevcudiyet, kütüphanelerde internet kullanımı ve kütüphanede yer alan basılı kaynakların elektronik ortama taşınmasıyla bilgi paylaşımını arttırmış ve hızlandırmış olsa da birçok tehdidi de beraberinde getirmesi verilebilir. Bu tehdit unsurları; kullanıcı sayısının çok olması, yetkisiz erişim girişleri ve kütüphane sistemindeyken yasal olmayan başka sitelere girerek kütüphane sistemine kötücül yazılım (virüs, solucan) bulaştırma (Öztemiz ve Yılmaz, 2013) gibi istenmeyen birçok duruma neden olabilir. Bu iki örnek bilgi güvenliğini birçok tehdit eden unsur olabileceğinin açık birer göstergesidir.

Kurumsal bağlamda düşünüldüğünde; bilgi güvenliğini tehdit unsurları kurum içi ve kurum dışı olmalarının yanı sıra kurumun bilgi kaynağının bulunduğu sistemlerden veya kurum

çalışanlarından da gelmesi mümkündür (Al-Awadi ve Renaud, 2007). Kurum bilişim sistemine yönelik bilgi güvenliği tehdit unsurları; kötücül yazılımlar (virüs, Truva atı, solucan vb.) olabileceği gibi reklam yazılımı, casus yazılım, tuş kaydediciler, araç çubukları (Çalışkan, 2014, s. 19-21) gibi unsurlar da olabilir. Bu unsurlar sistemin işleyişini engellemek, veri akışını azaltmak, sisteme erişimi engellemek hatta sistemdeki bilgilerin başka bir sisteme aktarılmasına gibi birçok olumsuz duruma da neden olabilir. Bilgi güvenliğini tehdit eden en önemli unsurlardan birisi ise kurum çalışanlarının eğitim ve bilinç düzeyindeki yetersizlik sonucunda meydana gelen durumlardır. Kurum çalışanlarına yönelik uygulanan sosyal mühendislik gibi yöntemler bilgi güvenliğini tehdit eden önemli unsurlar arasında yer alır. Sosyal mühendislik birçok yöntemi barındırır. Omuz sörfü taktiği ile sistem içindeki yetkili kullanıcının onun haberi olmadan gözlemlenip şifre bilgilerinin ele geçirilebilmesi, güvenini kazanarak yasa dışı bilgi edinme, oltalama (Keskin ve Gözenman, 2019, s. 291) gibi yöntemler bunlardan bazılarıdır. Bu tehdit unsurlarının temelini de güvenliğin en zayıf halkası olan insan üzerinden yapılması dikkat çeken konulardan biridir. Bu tehdit unsurlarına karşı bilgi güvenliğinin en zayıf halkası olan insanın en güçlü halkaya dönüştürülmesi muhakkaktır (Pfleeger, Sasse ve Furnham, 2014). Kısacası, artan bu tür tehditlere karşı çalışanların farkındalık düzeylerinin ve buna bağlı koruyucu davranışların artırılması (Jansson ve von Solms, 2013) da oldukça önemlidir.

Bu tehdit unsurlarına karşı, hem teknolojik açıklar kapatılmalı hem de insan faktörünün farkındalık faaliyetleri yükseltilmelidir. Bu kapsamda yapılması gerekenler aşağıda sıralanmıştır:

- Önem derecesine göre; bilgi, siber uzayda paylaşımı, iletimi, depolanması durumunda şifrelenerek (kriptolanarak) koruma altına alınmalıdır (Yerlikaya, Buluş ve Buluş, 2006). Kriptolama işlemi ile bilgi yetkisiz kişilerce erişilemeyeceğinden gizlilik, yetkili kişilerce ulaşılabileceğinden erişilebilirlik, istenmeyen değişimlere maruz kalmayacağından da gizlilik unsuru sağlanmış olur.
- Bilgi sistemlerine kurulan güvenlik duvarları (Firewall) sayesinde istenmeyen bilgi trafiği filtrelenmiş olur. Bu sayede sistemde istenmeyen olumsuz bilgi akışının önüne geçilerek emniyet unsuru sağlanmış olur (Karaarslan, 2003).
- Bilgi trafiği ve bu trafikte neler olduğunun gözlemlenmesi için kayıt tutulması ve bilgilerin yedeklenmesi oldukça önemlidir. Yedekleme sayesinde kritik öneme sahip bilgiler, yapılan veya yapılacak olan siber saldırılara karşı korunarak bütünlük unsuru

sağlanır (Aslan, 2019). Bilgi trafiğinin kayıt altına alınması da sisteme yetki erişimi bulunan kişilerin yaptıkları veya yapacakları yasa dışı faaliyetleri inkâr edememelerini sağlamış olur. Log adı verilen bu kayıtlar sayesinde hesap verilebilirlik, inkâr edememe, denetlenebilirlik, emniyet gibi birçok bilgi güvenliği unsuru koruma altına alınmış olur.

- Bilginin üretiminden yok edildiği ana kadar olan sürecin takibi için bilgiye yapılacak sayısal damgalama işlemi ile bilginin izlenmesi sağlanabilir (Emek, 2006). Bu durum sayesinde siber uzayda varlık gösteren bilgi izlenebilir. Böylece bilginin denetlenebilirlik, gizlilik unsurları da sağlanmış olur.
- Antivirüs programları sistem içerisinde yer alan bilginin, zarar görmesini önlemek için önem rol oynar (Çakır ve Kesler, 2012). Bu programlar sayesinde bilgiye zarar verecek virüs, solucan vb. kötücül faaliyetleri tespit ederek bilgiye verilecek zararları önler. Bu sayede bilginin bütünlük unsuru korunmuş olur.
- Saldırı önleme ve saldırı tespit etme sistemleri olan IPS/IDS, sistemlerde meydana gelen veya gelebilecek tehlikeleri tespit etme ve bunların zararlı etkilerini yok etmeyi sağlar (Papadaki ve Furnell, 2004). Bu sistemler sayesinde bilgi güvenli bir ortamda varlık göstererek emniyet ve güvenilirlik unsuru sağlanmış olur.
- Bilgiyi koruma altına almada, yetkili kişilerin yetki dâhilinde bilgiye ulaşmasında kişinin sistemde tanınmasını sağlayan kişiye şifre/parola verilmesi veya parmak izi, retina, yüz taraması gibi biyometrik özelliklerinin sisteme girmek için onaylanması gibi yöntemler kullanılabilir (Aladağ, Kurtarangel ve Bahtiyar, 2014). Bu sayede yetkisiz kişilerin bilgiye erişimi engellenmiş olur. Ayrıca bilgiye ulaşmak için kişi kimliğini de doğrulamış olur. Bu nedenle kimlik doğrulama unsuru da sağlanmış olur.
- Sosyal mühendislik yöntemi, güvenliğin zayıf halkası olan insan faktörüne odaklanarak bilgi güvenliğini tehlikeye atıp en güvenli sistemlere bile yetkisiz kişilerin erişimini sağlar. Sosyal mühendislik, temel olarak insanın zafiyetlerini kullanarak yetkisi olmayan bilgiye erişimi amaçlar. Korku, yardım etme isteği, dikkatsizlik ve rahat bölge düşüncesi sosyal mühendislikte insan zafiyeti olarak kullanılan duygulardır (SANS, 2004). Yemleme (phishing), omuz sörfü, çöp kurcalama vb. yöntemler ve kişilerden elde ettiği bilgilerle yetkisi olmayan bilgiye erişim sağlamış olur (Irmak ve Reis, 2018). Bu durum neticesinde bilginin gizlilik, güvenlik ve bütünlük unsurları ihlal edilerek bilgi güvenliği tehlikeye girmiş olur.

2.1.4. Bilgi güvenliği farkındalığı kavramı

Bilgi güvenliğinin öneminin artması neticesinde, güvenliğin nasıl sağlanacağı konusunu gündeme gelmiştir. Bilgi güvenliğinin sağlanması için iyi bir organizasyon, teknoloji ve farkındalık sürecinin işletilmesi gerekir (Erol, Ceylan ve Sağıroğlu). Siber uzay ve gerçek dünya arasında köprü olan insan bu süreçte etkin bir rol oynamakta ve bu hususta farkındalık kavramı, incelenmesi gereken konulardan biridir. Bilgi güvenliği kavramı için kişilerin uyması gereken kurallar ile ne tür politika ve prosedürler uygulamaları gerektiği üzerine sergilenecek tutum ve davranışlar, bilgi güvenliği farkındalığını oluşturur (McCormac, Zwaans, Parson, Calic, Butavicius ve Pattinson 2017, s. 151). Bilgi güvenliği farkındalığı, bilgi güvenliği için kuruluşun veri ve ağını korumaya yönelik kontrol mekanizması konumundadır (Shaw, Chen, Harris ve Huang, 2009, s. 92). Kısacası bilgi güvenliği farkındalığı, bilgi güvenliği konusunda güvenlik halkasının en zayıf faktörü olan insanın (Tsohou, Karyda ve Kokolakis, 2015; Jeimy ve Cona, 2019) yaptığı faaliyetler sonucunda ortaya çıkan sorumluluğun anlaşılması için geliştirilmiş bilinçlendirme faaliyetlerinin tamamıdır.

Temelde bilgi güvenliği, bilginin temel unsurları olan gizlilik, bütünlük, erişilebilirliği muhafaza etmeye yönelirken; bilgi güvenliği farkındalığı, bilgi güvenliği için etkin bir ortam oluşturarak bilgi güvenliğinde devamlılığı esas kılan bilinçlendirme programlarını oluşturmayı amaçlar (Kruger ve Kearney, 2006). Bu nedenle bilgi güvenliği farkındalığı aslında bilgi güvenliğinin koruyucusu görevini üstlenerek insan faktörüne yönelik yürütülen faaliyetlere odaklanmaktadır. İnsan, bu süreçte sadece güvenliğin en zayıf halkası olarak değil aynı zamanda gerçek ortam ve siber uzay arasında yaptığı eylemlerle nüfuz etme kapasitesine sahiptir. Bu nedenle bilgi güvenliği farkındalık kavramının temelini oluşturmaktadır. Kısaca, bilgi güvenliği farkındalığı, insan faktörünü bu sürece en zayıf halkadan en güçlüye dönüştürmeyi hedefleyen ve bilgi güvenliği için olmazsa olmaz unsurlardan biridir (Marşap, Akalp ve Yeniman, 2010).

2.1.5. Bilgi güvenliği kültürü ve bilgi güvenliğinde insan faktörü

Ham verinin işlenmesi ile ortaya çıkan bilginin zaman içerisinde siber uzaya taşınması neticesinde bu ortamda karşılaşılabileceği tüm tehditlere karşı korunması için bilgi güvenliği kültürü ve bilgi güvenliğinde insan faktörünü kapsayan durumlar oldukça önemlidir (Aktan ve Aydın, 2016). Bilgi güvenliği, bilginin var oluşuyla beraber ortaya çıkan bir sorundur

ancak bilginin siber uzaya taşınması bu sorunun daha çok gündeme gelmesini sağlamıştır. Bilgi güvenliği kültürü ve insan faktörünün bilinçlendirilmesi, siber uzayda bulunan bilginin güvende kalması için yürütülen bir takım faaliyetleri içermektedir.

Bu faaliyetlerin başında, bilgi güvenliği kültürü gelmektedir. Bilgi güvenliği kültürü; çalışan bireylerin işyerindeki davranışlarını etkileyen kurum kültürünün bir kısmını oluşturmaktadır (Acılar, 2009, s. 30). Bu nedenle bilgi güvenliği kültürü, doğası gereği kurumsal veya örgütsel biçimde ele alınmalıdır (Reid ve Niekerk, 2014). Bilgi güvenliği kültürü bir kurum kültürü yapısına ihtiyaç duymaktadır ve zaten örgüt kültürü öğrenilen davranışları kapsayan bir sistemi yansıtmaktadır (Aktan ve Aydın, 2016). Siponen'in (2000), Connolly, Lany, Gathegi ve Tygar'ın (2017), Hu, Dinev, Hart ve Cooke'n (2012) yaptıkları çalışmalarda; örgüt kültürünün, çalışanları bilgi güvenliği davranışı sergilemeye teşvik ederek onları motive ettiği belirtilmiştir. Bilgi güvenliği kültürü, aynı zamanda bilgi varlığına tehdit oluşturacak davranışlarından uzak durmak için çalışanlara bilgi teknoloji hizmetlerini kullanırken kılavuzluk yapmaktadır (Erbil, 2018, s. 47). Bilgi güvenliği kültürü, teknik olarak ele alınan tüm sosyo-kültürel güvenlik yöntemlerini de kapsamaktadır (Schlienger ve Teufel, 2003, s. 405). Kısacası bilgi güvenliği kültürü, bilginin güvende olması için çalışanlara güvenlik davranışı kazandırmak için bilgi varlığı ve insan arasında oluşan etkileşime yön veren her türlü değer, algı, olasılıklarla bilgi toplanmasının sağlamaktadır (AlHogail, 2015, s. 567). Bilgi güvenliği kültürünün oluşmasının temelini, bilgi sistemleri ile temas eden insanların bu kültüre dâhil edilmesi ile mümkündür. Bu nedenle bilginin güvende olması ve bilgi toplumu olabilmenin önemli şartlarından biri bilgi güvenliği kültürünün oluşturulması (Altın ve Görgün, 2014) ve insanın bu sürece dâhil edilmesidir.

Bilgi güvenliği kültürünün oluşturulmasında insan faktörünün nasıl konumlandırılacağına anlaşılması oldukça önemlidir. Kurumsal olarak bilgi güvenliği doğası gereği insan, teknoloji, çevre ve örgüt faktörlerine bağlı bir yapıda gelişebilir (Wachira, 2021, s. 8). Bilgi güvenliği zincirinin en zayıf halkası olarak görülen insan (Tsohou, Karyda ve Kokolakis, 2015; Jeimy ve Cona, 2019) alanyazında bu hususta çeşitli benzetmelere maruz kalmıştır. İnsan faktörü, bilgi güvenliği işleyişinin savunmasız tarafı (Tamjidyamcholo, Baba, Tamjid ve Gholipour, 2013), bilgi güvenliği için saldırılarda istismar edilen öge (Khan, Alghathbar, Nabi ve Khan, 2011), aşıl topuğu (Gonzalez ve Sawicka, 2002) ve direk ilişkili bir değer (Alotaibi, Furnell ve Clarke) olarak görülmektedir. Bu nedenle bilgi güvenliğinin sağlanması ve bilgi güvenliği kültürünün oluşturulmasında, insana yatırım yapılmalı ve insanı etkileyen tüm faktörler ele alınarak bütüncül bir yaklaşım sergilenmelidir. Bilgi güvenliği için insan

faktörünün oluşturulmasında katkı sağlayan iki unsur mevcuttur ve bunlar (Van Niekerk ve Von Solms, 2005):

- Bilgi güvenliğinin etkili bir biçimde uygulanması ve kontrol mekanizmasının iyi anlaşılması için kurum çalışanlarına yeterli bilginin verilerek konu hakkında bilgi sahibi olmalarının sağlanması gerekir.
- Bilgi güvenliği politikalarının anlaşılması için, kurum; çalışanlarının farkındalık düzeyini arttırarak onları doğru davranış sergilemeye yönlendirilmesi gerekir.

Bu iki unsur, bilgi güvenliği kültürünün oluşturulmasında insan faktörünün sürece nasıl dâhil edileceği hakkında fikir vermektedir.

2.1.6. Bilgi güvenliği ile ilgili ulusal ve uluslararası alanda yapılan etkinlikler

Bilginin varoluşundan beri geçirdiği dönüşüm sonucu meydana gelen güvenlik ve tehdit kavramlarının sonucunda gerek ulusal gerek uluslararası birçok çalışma yürütülmüş ve yürütülmeye devam etmektedir. Bilgi güvenliği hakkında yürütülen çalışmalar incelendiğinde aşağıda çalışmalara rastlanmaktadır:

- İlk kez 1997 yılında düzenlenen Uluslararası Bilgi Güvenliği Çalıştayı (Information Security Workshop (ISW)) 1999 ve 2000 yıllarında da yapılmıştır. Daha sonra 2001 yılında Bilgi Güvenliği Konferansı (Information Security Conference (ISC)) adı altında yapılmaya devam etmiştir (İnternet, Springer Link, 2021). Bu yıl 9-13 Kasım'da 24.sü Endonezya'da gerçekleşmiştir (ISC, 2021).
- Finansal Hizmetler Bilgi Paylaşımı ve Analiz Merkezi (Financial Services Information Sharing and Analysis Center (FS-ISAC)) CERES Forumu ise finans sektöründe bulunan merkez bankası, düzenleyici ve denetleyici kuruluşlar için sanal ortamda meydana gelebilecek saldırılar için çözüm yolları arar (İnternet, FS ISAC,2021).
- İlk faaliyet yılı 2003 olan Hack in the Box Güvenlik Konferansı (HITBSECCONF), yeni nesil bilgi güvenliği üzerine dünya çapında birçok araştırmacıyı ağırlamaktadır. 23-27 Ağustos 2021 tarihlerinde çevrimiçi olarak “*Uygulamalı Teknik Eğitimler ve Çift Hatlı Güvenlik*” temalı konferansı gerçekleştirecektir (İnternet, HITBSecConf, 2021).

- Açık Web Uygulama Güvenliği Projesi (Open Web Application Security Project (OWASP)) tarafından uluslararası alanda yıllık olarak düzenlenen Küresel AppSec Konferansı bilgi güvenliğini korumanın bilginin bulunduğu sistemlerdeki yazılımın güvenli hale getirilmesi (İnternet, OWASP, 2021) ile mümkün olacağını ifade ederek bu konferansı düzenlemektedir.
- Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency (ENISA)) tarafından desteklenen önemli etkinliklerden biridir. Bu etkinlik her yıl belirlenen ana tema çevresinde birçok akademisyeni bir araya getirmektedir. Kısaca ISC Turkey olarak bilinen konferansın 2019 yılında 12.si düzenlenmiştir ve Avrupa Siber Güvenlik Ayı etkinlikleri arasında yer almıştır. 13. ISC Turkey 3-4 Aralık 2020 tarihinde düzenlenmiş konferansın ana teması “*Siber Güvenlik ve Güvenli Veri Paylaşımı*” (İnternet, ISC Turkey, 2021) olmuştur.
- Bilgi Sistemi Derneği (Association for Information System (AIS)) tarafından ilk 1980 yılında yapılan Uluslararası Bilgi Sistemleri Konferansı (International Conference on Information Systems (ICIS)) akademisyen ve araştırmacılar için ilgi odağı olmuştur (İnternet, AIS, 2021).
- Bazı etkinlikler bölgesel düzenlenmiştir. Bunun en iyi örneklerinden birisi de InfoSecurity Avrupa Konferansıdır. Bu konferans, 13-15 Temmuz 2021 tarihleri (Infosecurity Europe, 2021) arasında düzenlenmiş olup bölgenin bilgi güvenliği ihtiyaçları belirlenmiştir.
- Bilgi güvenliği üzerine ulusal etkinlikler de mevcuttur. I. Ağ ve Bilgi Güvenliği Sempozyumu ilk olarak 2005 yılında gerçekleştirilmiştir. Bu sempozyumun temel amaçlarından biri, özellikle bilginin barındığı ağ ortamındaki güvenlik üzerine yaptıkları çalışmalarla öncülük eden birçok akademisyen ve araştırmacının çalışmalarını sunarak tartışmalarıdır (İnternet, Elektrik Mühendisleri Odası, 2005). Bu sempozyumun sonuncusu 2011 yılında gerçekleştirilmiştir (Canbek, Sağıroğlu ve Baykal, 2013).
- Bir başka ulusal etkinlikte 2009 yılından başlayarak her yıl düzenli yapılan ve sonuncusunun 2019 yılında yapıldığı İstanbul Bilgi Güvenliği Konferansı (İscSec) olmuştur. Bu konferans bilgi başta olmak üzere ağ ve sistem yöneticilerinin yanı sıra etik hacker olmak isteyen kişilere yönelik hazırlanmış içeriğe sahip konferanstır (İnternet, BGA Güvenlik, 2019).

Tüm bu uluslararası, bölgesel ve ulusal etkinliklerin amacı; bilgiyi içinde barındıran sistemleri daha güvenilir hale getirerek bilgi güvenliğini tehdit eden unsurlar karşısında risk analizi oluşturarak gerekli tedbirlerin alınmasına yardımcı olmaktır. Tüm bunları yaparken insan faktörünü bilinçlendirmeye odaklanır.





3. ADLİ BİLİŞİM VE KURUMSAL BİLGİ GÜVENLİĞİ FARKINDALIĞI

3.1. Kurumsal Bilgi Güvenliği ve Farkındalığı

Kurumsal bilgi güvenliği farkındalığı oluşturmak için kurumsal bilgi güvenliği, standartları ve yöntemlerinin anlaşılması gerekmektedir. Bu kısımda, kurumsal bilgi güvenliği ve farkındalığına katkı sağlayacak standart ve yöntemlerden bahsedilecektir.

3.1.1. Kurumsal bilgi güvenliği

Kurumsal bilgi güvenliği, bilgi güvenliğinin kapsama alanı içinde yer almaktadır. Bilginin gönderildiği kaynaktan alıcıya gidene kadar herhangi bir değişime uğramadan güvenli bir şekilde iletilmesini ifade ederken kurumsal bilgi güvenliği ise bu durumun kurumsal olarak gerçekleşme durumunu ifade etmektedir. Bu nedenle kurumsal bilgi güvenliği; kurum içindeki güvenliğin sağlanması için belirli seviyedeki güvenlik politikalarının, çalışan bilişim personeli ve onların bağlantıda bulunduğu diğer kurumların uyması gereken kuralların tümü olarak ifade edilebilir (Kalman, 2003, s. 60). Kurumun bilgi güvenliği devamlılığının esas olabilmesi için kuruma ait olan bilgi ve bilgi varlıklarının güvende olması gerekir (Mitchell, Marcella ve Baxter, 1999). Bilgi varlıklarının güvende olması için de bilgi güvenliği unsurlarının sağlanması gerekir.

Bilgi güvenliğinin temel unsurları, tıpkı bilgi güvenliği gibi kurumsal bilgi güvenliğinin de temelini oluşturur. Bununla birlikte kurumsal çerçevede aktarılan, depolanan veya kontrol altında tutulan bilginin bütünlüğü, gizliliği ve erişilebilirliğinin korunabilmesi için kayıt tutma, kimlik doğrulama, sorumluluk, erişim denetimi, inkâr edememe, güvenilirlik ve emniyet (Çağlayan, 2003, s. 5) gibi unsurların temel unsurlara eşlik etmesi gerekir. Kurumsal bilgi güvenliğinde çalışanların nerede, ne zaman, kim tarafından, hangi işlem ile bilgiye müdahale edildiğini bilmek kurumsal bilgi güvenliğinin sağlanması için önemli bir adımdır. Sonuçta kurumsal bilgi güvenliği; teknoloji, insan ve yönetim prensiplerindeki unsurların bir araya gelerek uyum içinde çalışması ile mümkündür (Vural, 2007). Kurumsal bilgi güvenliğini sağlamak için bir kurumda; kurumsal bilgi güvenliği politikası, bilgi güvenliği yönetimi ve standartların olması gerekir (Vural ve Sağıroğlu, 2008).

Kurumsal bilgi güvenliği politikası

Kurumsal bilgi güvenliği politikası, kurum ve kuruluşlar için bilgi güvenliği devamlılığının sağlanabilmesi için tüm bilişim alt yapı güvenliği de dâhil olmak üzere başka güvenlik faaliyetlerini de içine alan talimatlar ile beraber kurumsal bilgiye erişim yetkisi bulunan bütün kurum çalışanlarının uyması gereken kurallardan oluşan sertifikalı belgelerdir (Vural ve Sağıroğlu, 2008, s. 508). Bu politika, kurum ve kuruluşlar için sağlanacak olan bilgi güvenliği faaliyetlerini içine alan ve kurumsal olarak bilgi erişimine sahip bütün kurum çalışanlarının uymakla yükümlü olacağı kuralların belirlendiği belgelerdir (Marşap ve diğerleri, 2010, s. 354). Kısacası bu politika, bilgi güvenliğinin sağlanması için alınacak tedbirlerin oluşturulduğu kurumsal faaliyetlerin yazılı olduğu belgelerdir (Karaarslan, Teke ve Şengonca, 2003). Bu nedenle kurumsal olarak bilgi güvenliğinin sağlanmasında kurumsal bilgi güvenliği politikasının rolü oldukça önemlidir. Alanyazında kurumlar için belirlenen bilgi güvenliği politikası çeşitli benzetmelere tabii tutulmuştur. Özden Aktaş, Karabağ, Uğur, Akyüz, Takçı ve Soğukpınar'a (2020) göre bilgi güvenliği politikası kurumun anayasası şeklinde görülürken, Thomson, Von Solms ve Louw'a (2006) göre bilgi güvenliği politikası resmi olarak bilgi güvenliğine bağlılık göstergesi olarak görülmüştür. Ayrıca Von Solms (2001)'e göre kurumsal bilgi güvenliği politikası, bilgi güvenliği için kişilere yetki veren bir referans durumudur. Mears ve Von Solms'a (2004) göre ise bilgi güvenliği politikası, bilgi güvenliğini tanımlamakla beraber üst yönetim ve kurulun desteğine sahip olan yön verici belgelerdir. Bu nedenle bu politikaların bazı özelliklere sahip olması gerekir. Bilgi güvenliği politikasının sahip olması gereken özellikler;

- Bu politikalar, kurumdaki üst düzey yönetim tarafından desteklenmelidir.
- Bu politikalar, kurum çalışanları tarafından benimsenmelidir.
- Bu politikaların uygulanmasının kolay olması için çalışanlar tarafından rahat anlaşılmalı ve bununla beraber yöneticilerin de bu politikaları kolay yönetebilmesi gerekir (Tekerek, 2008)
- Bu politikalar, kurumsal bilgi güvenliği yönetimi için belirli standart ve prosedürleri içermelidir.
- Bu politikaların anlaşılıp kolay uygulanması için kısa ve anlatımı yalın olmalıdır (Bingöl, 2010).
- Bu politikalar kurumun ihtiyaçları doğrultusunda geliştirilmeli ve dönüştürülmelidir.
- Bu politikalar ISO 27001:2013 (ISO,2021) standardına uygun olarak kurumun ihtiyacı doğrultusunda belirlenmeli ve zaman içerisinde geliştirilmelidir.

Tüm bu özellikler benimsenen bilgi güvenliği politikasına dinamiklik katarak bu politikanın ihtiyaçlar doğrultusunda kendini yenilemesine imkân sağlamasına yardımcı olmaktadır. Unutulmamalıdır ki teknoloji sürekli değişmektedir ve bu değişime bağlı olarak siber uzayda bulunan bilginin güvende kalma koşulu da değişmektedir. Bu nedenle belirlenecek kurumsal bilgi güvenliği politikası bu değişimlere ayak uydurarak kurum çalışanlarının konu hakkındaki taleplerini karşılaması gerekir ancak bu şekilde etkin bir politika olarak varlık gösterebilir (Alagöz ve Allahverdi, 2011).

Kurumsal bilgi güvenliği yönetim sistemi ve standartları

Kurumsal bilgi yönetiminin doğru sağlanması kurumsal bilginin güvenliği yönetimine yardımcı olur. Kurumsal bilgi yönetimi, kurumsal işleyişte üretilen her türlü bilginin etkin biçimde depolanıp kurumun hedef ve stratejileri doğrultusunda kullanılması sürecini kapsar (Semiz ve Tüfekçi, 2019, s. 236). Kurumsal bilgi güvenliğinin sağlanması için iyi bir kurum politikasının yanı sıra iyi bir kurumsal bilgi yönetimi de gereklidir. Kurumsal bilgi yönetiminin sağlanması kurumsal bilgi güvenliği yönetimi için ilk adım niteliğindedir ancak tek başına yeterli değildir. Kurumsal bilgi güvenliği yönetiminin sağlanması için kurumsallaşmanın getirdiği bazı standardizasyon faaliyetlerinin anlaşılması önemlidir. Kısacası kurumsal bilgi güvenliği hem kurumsal bilgi yönetimine hem de standardizasyon faaliyetlerine bağlıdır.

Kurumsal bilgi güvenliği standardizasyon faaliyetleri için dünya genelini kapsayacak şekilde ve kurumları ortak paydada buluşturacak standartlaştırma çalışmaları mevcuttur (Akcan, 2019). İlk olarak BS-7799 standardı, Uluslararası Standardizasyon Örgütü (ISO) tarafından kurumsal varlıkların ve bunlara yönelik güvenlik tehditlerinin belirlenmesi için yapılan risk analizi ve güvenlik kontrolünde oluşturulmuştur (Kenning, 2001). Bu standardın adı ISO/IEC 17799:2005 iken 2007 yılında ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi (BGYS) adını almıştır ve 2013 yılında ISO tarafından revize edilmiştir (Gencer, 2015). ISO/IEC 27001 standardı; kurumlardaki risk yönetim planları ve bu yönetim planları ile beraber risk işleme konusunda yapılacak görev ve sorumlulukların yanı sıra işin devam edebilmesi için gerekli faaliyetleri kapsamaktadır. Kurumda acil durumların olabileceği göz önünde bulundurularak acil durum olay yönetimi ve konuyla ilgili prosedürlerin belirlenerek uygulanmasında için bunları kayıt altına almalıdır. Kurum, yukarıda belirtilen tüm konu başlıkları için bir bilgi güvenliği politikası belirleyerek standarda uygun olarak bunu kurum çalışanlarına bildirmeli ve çalışanları bu konuda eğitmelidir. Bu sürecin aksamadan

ilerlemesi; süreç hedefleri ölçülmeli ve gerçekleştirilen performansların daimi olarak takip edilmesi ile beraber kurum çalışanlarının tümünün bu sürece dâhil edilmesi ile başarıya ulaşabilir (Denerel, 2016). Kısacası bu standart, kurumun bünyesinde bulundurduğu BGYS'nin kurulması ile beraber kurulan bu sistemin işletilmesi ve sistemin sürekliliğinin sağlanması için yapılması gerekenleri belirlemektedir.

Bilgi güvenliği yönetim sistemi ise; artan bilgi paylaşım ortamındaki tehlikelerin sadece teknoloji tabanlı (virüs, kötücül yazılım, casus yazılım vb.) değil aynı zamanda kişilerin süreç içerisindeki yanlış tutum ve tavır neticesinde de kaynaklanmasından ötürü teknoloji, insan (şifre gizliliği, disk paylaşımı vb.) ve prosedürleri de içine alan kurumdaki üst yönetimin desteği ile tüm çalışanların uyması ve uygulaması gereken bir yönetim sistemidir (Yılmaz, 2014, s. 51). Kısacası bilgi güvenliği yönetim sistemi; kurumda oluşan tüm bilginin bilgi güvenliğinin üç temel unsuru olan; gizlilik, bütünlük ve erişilebilirlik ilkeleri ile uyumlu olarak kurallara uygun biçimde sistemsel ve planlı olmakla beraber yönetilebilen ve bu yönetimin sürdürülebilir dokümantasyonu yapılmış uluslararası güvenlik standartlarına uygun üst yönetimin kabul ettiği faaliyetlerin tümüdür (Ersoy, 2012, s. 8). Bu kapsamlı yönetim sisteminde bilişim sistemleri ve onlarla temas halinde bulunan kurum çalışanlarının entegrasyonu kurumsal bilgi güvenliğini sağlamak için temel unsurlardan biridir. Bu nedenle BGYS'nin amacına ulaşabilmesi için dört aşamalı; planla, uygula, kontrol et ve önlem al (PUKÖ) süreçlerinden geçmesi gerekir (Gazdağı ve Çetinyokuş, 2020). İlk aşama olan *planlama* aşamasında risk yönetimi aşamalarını belirleyecek BGYS'deki hedef, prosedür ve proseslerin belirlenmesini hedef alırken ikinci aşama olan *uygulama* aşaması ise planlama aşamasında oluşturulan politikadaki kontrol, süreç ve prosedürlerin hayata geçirilerek işleme sokulmasını sağlar. Üçüncü aşama olan *kontrol etme* aşamasında daha önce tecrübe edilen kontroller için proses performansı değerlendirilmesi ile uygulanan yerlerdeki ölçümlerin incelenerek raporlanmasını sağlarken dördüncü ve son aşama olan *önlem alma* aşaması da kaynak devamlılığı için düzeltici ve koruyucu önlemleri ele almaktadır (Mete, 2010).

Kurumsal bilgi güvenliği için kurumsal bilgi güvenliği yönetimi ve standartlarının çeşitli yararlarını sıralamak gerekirse (Demirtaş, 2013, s. 50):

- Standartların uluslararası geçerliliği bulunduğundan bilgi güvenliği yönetimini bu standartlar oluşturduğu için birçok farklı kurum ve kuruluşa uygulanabilir.
- Kurum ve kuruluşlar için gerek yönetim gerek teknik vb. alanlarda güvenlik için geniş bir bakış açısı sunabilir.

- Güvenlik için gerekli yasal çerçevelere uygun olduğundan kurum ve kuruluşlara yasal uyum yeteneği sunar.
- Kurum ve kuruluşlara standartlaşmanın getirdiği itibarın yanı sıra iş alanında çalışılan diğer paydaşlara güven duygusu aşılar.
- Kurum ve kuruluşların bünyesinde çalışan kişilere karşı üst yönetimin sorumluluk odaklı olmasını sağlar.

3.1.2 Kurumsal bilgi güvenliği farkındalığı ve insan faktörü

Bilgi güvenliği ve bilgi güvenliği kültüründe olduğu gibi kurumsal bilgi güvenliği farkındalığında da insan faktörü oldukça önemlidir. Bilgi güvenliği farkındalığının temelini; insan ve insanların uyması gereken güvenlik politikaları oluşturmaktadır. Sonuçta bilgi güvenliğinin sağlanabilmesi doğru planlara, güçlü güvenlik tedbirlerine ve çalışan insanların farkındalık seviyesinin yüksek olması ile mümkün olabilir. İnsan gerçeklik ve siber uzay arasında geçiş kapısı görevi üstlendiği (Nezgitli, 2021) için kurumsal bilgi güvenliği farkındalığının gerçekleşmesi de yine kendisine bağlı bir durumdur. Saldırı ve saldırı biçimlerinde açık bulma arayışı güvenliği en zayıf halkası olan insan faktörü üzerinden devam ettirilmektedir. Birçok saldırı senaryosu insanın bilgi güvenliği farkındalığının yetersizliğinden meydana gelmektedir. Kurum, bilgi güvenliğine yönelik tehditler karşısında insan faktörüne eğilmeli ve insanların farkındalık düzeyini arttırmalıdır. Bu farkındalık düzeyi; çeşitli eğitimler (Dhillon, 1999), programlar (Kraus, 2018) ve kursların (Hutinski, Kisasondi ve Bambir, 2009) sonucunda insanlar sistemlerde yetkili erişime sahip olmaları gerekir. Bu nedenle kurumsal bilgi güvenliği farkındalığının temelini insan faktörü oluşturduğu için yapılacak yatırımlar da insan farkındalık düzeyini arttırmaya yönelik olmalıdır (İnternet, Doğan, 2021). Kurumsal bilgi güvenliği farkındalığı konusunda, çalışan kişilerin dikkatsiz ve bilinçsiz olarak yapacakları en ufak hatalar bile kurum için maddi ve manevi geri dönüşü olmayan sonuçlara neden olabilir. Bu nedenle özellikle insan faktörü düşünülerek farkındalık düzeyini oluşturmak için belirli yöntemler uygulanmalıdır. Bu yöntemlerdeki temel amaçları aşağıda sıralanmıştır. Bunlar (Şahinaslan ve diğerleri, 2009):

- Bilgi güvenliği konusunda tüm çalışanlara yönelik eğitim ve farkındalık programları kurumun ihtiyaç duyduğu doğrultuda gerçekleştirilmelidir.
- Verilen bu eğitimler ve programlar kurum çalışanlarının ihtiyaçları ve teknolojiadaki değişiklikler karşısında yenilenmeli ve bu eğitimler düzenli bir şekilde verilmelidir.

- Eğitim ve programın içerikleri yüz-yüze ve çevrim içi olabileceği gibi çalışanlara verilecek el kitapçıkları, belirli aralıklarla düzenlenen etkinlikler ve bilinçlendirme çalışmaları şeklinde de olabilir.
- Çalışanların günlük iş temposundaki yoğunluğu karşısında dikkat dağınıklığının artabileceği düşünülerek ekran koruyucu vasıtasıyla bilgi güvenliği farkındalığı hakkında belirli aralıklarla mesajlar iletilebilir.
- Kurumsal iletişim portalından kurum çalışanlarına yönelik kısa bilgi notları ve bilgi güvenliği hakkında hatırlatıcı önemli uyarılar yayınlanabilir.
- Verilen eğitimler sonrası, çalışanların bilgi güvenliği farkındalık düzeylerini anlamak için kurumun geri bildirim alabilecekleri bir değerlendirme mekanizmasına sahip olması gerekir (AlMindeel ve Martins, 2020).

Tüm bunlar kurum çalışanlarını bilgi güvenliği için daha bilinçli olmasını sağlayarak bilgi güvenliği farkındalığı yüksek bireylerin oluşmasını sağlayacaktır.

3.1.3 Kurumsal bilgi güvenliği farkındalığı ve kültürü

Bilgi güvenliğinin oluşması için sağlanacak olan bilgi güvenliği kültürü gibi bilgi güvenliği farkındalığının oluşması için de bilgi güvenliği farkındalığı kültürünün oluşturulması için kurumsal yapılanma oldukça önemlidir. Sonuçta oluşturulacak bu farkındalık için bir örgütlenme yani organize olan bir insan topluluğu gereklidir (Acılar, 2009). Gereken bu topluluk belirli bir amaç için organize olmalıdır ve belirli kurallar çerçevesinde bir araya gelmelidir (Gürüz ve Gürel, 2006). Bu nedenle bilgi güvenliği farkındalığı ve bunu oluşturacak bir kültür oluşturulması için kurumsal bir yapılanma gereklidir. Kurumsal bilgi güvenliği farkındalığı kültürü için tüm kurum çalışanlarının oluşturulan bu kültüre uyum göstermesi için bilinçlendirilmesi ve belirli faaliyetlerle konuyu anlayarak uyum içinde çalışmaları gerekmektedir. Bu sürecin kalıcı olması için de edinilen bu kültürün devamlılık esası ile hareket etmesi ve kurum çalışanları değişse bile yeni çalışanlar ile beraber sürecin kaldığı yerden devam etmesi gerekmektedir. Kısaca kurumsal bilgi güvenliği kültürü için belirli kurallar, organize olmuş insan topluluğu, devamlılık esas alınacak üç ana esastır. Bu esaslar ile beraber kurumsal bilgi güvenliği farkındalığı kültürü aslında kurumun zaman içerisinde oluşturduğu kendi kültüründen de belirli özellikler taşımaktadır (Gürsel, 2019). Taşıdığı kurum kültürü ile kurumun bilgi güvenliği ve bilgi güvenliği farkındalığı kültürü aralarında uyum gösterirse kurumsal başarı da sağlanmış olur. Bu nedenle gerek kamu gerek ise özel sektör için bilgi güvenliği ve bilgi güvenliği farkındalığı bir kültür olarak

görülmelidir (Tuluk ve Seferoğlu, 2016) ve oluşturulan bu iki kültüründe devamlılığı sağlanarak sürdürülmelidir ancak bu şekilde kurumsal bilgi güvenliği sağlanabilir.

3.2. Kurumsal Bilgi Güvenliği Farkındalığında Adli Bilişimin Rolü

Bilgi güvenliği üzerine yapılan yasa dışı faaliyetler bilgi iletişim teknolojilerinin hayatımıza girmesi ile farklılık göstermiştir. Bu yasa dışı faaliyetler, ilk olarak bilgisayarlar vasıtasıyla yapıldığı için *bilgisayar suçu* (Charney ve Alexander, 1996) adını alırken teknolojiye ilerlemeler ile beraber farklı cihazlar ve farklı yöntemler ile de işlenmeye başlanmış ve bu kavram yetersiz kalmıştır. Bu kavram, yerini zamanla *bilişim suçu* kavramına bırakmıştır. Birçok farklı çalışmada bilişim suçu; . Bilişim suçu, kişinin teknoloji bilgisini yasa dışı faaliyetlerde kullanarak işlediği suç olarak tanımlanmaktadır (Eriksson, 2018, s. 50). Bir başka tanımda, bilişim suçu; bilişim sistemlerindeki verilerin hedef alınarak güvenlik ve bütünlük unsurunu ortadan kaldıracak şekilde işlenen yasa dışı faaliyetler olarak tanımlanmıştır (Açıkgöz, 2020, s. 17). Kısacası, bilişim suçu; sadece bilgisayarlarla değil tüm teknolojik cihazlar kullanılarak bilginin gizlilik, bütünlük, erişilebilirlik gibi temel unsurlarının ihlal edilerek gerçekleştirildiği tüm yasa dışı faaliyetlerdir.

Bilişim suç tarihine bakılacak olunursa; dünyada ilk bilişim suçu, 1966 yılında 23 yaşında bilgisayar programcısı olarak çalışan bir banka çalışanının mevduat hesabında değişiklik yapmasıdır (Parker, 1968). Türkiye’de ise 1990 yılında ilk kez bir bilişim suçu mahkemece kayıt altına alınmıştır (Bilişim Ajandası, 2011). 1991 yılında Türk Ceza Kanunu’nda ilk kez “Bilişim Alanında Suçlar” başlığı altında düzenlenmiştir (Yazıcı, 2021). Teknolojinin ilerlemesi ile bilişim suçları artış göstermektedir (Brenner, 2004). Bu artış, Adli bilişime konu olan vakaları ve davaları da arttırmıştır. Bilişim suçlarıyla alakalı 2020 yılında 17.790 kamu davası açılırken, 2021 yılında 19.947 kamu davası açılmıştır ve açılan dava sayısında artış yaşanmıştır (İnternet, Adalet İstatistikleri, 2020-2021). Gökçearslan, Nezgıtlı ve Çakır’ın (2020) çalışmasında, genel olarak yıllar ilerledikçe gazetelere konu olan *bilişim suçu* haber sayısında da artış yaşandığı belirtilmiştir.

Bilişim suçlarının bilgi güvenliğine yönelik oluşturduğu tehditler karşısında bilgi güvenliğini sağlama ve suç faaliyetlerinin önüne geçmek için Adli bilişim önemli bir rol oynamaktadır. Sonuçta adli bilişim sayesinde; işlenen suçların, hangi cihaz ve yöntem kullanılarak işlendiğinin bilinmesi ve suçun doğru analiz edilmesi suçu işleyen kişi ve kişilerin yakalanmasına yardımcı olurken aynı zamanda suç işleme tekniklerinin bilinmesine de yardımcı olmaktadır. Adli bilişim; işlenen bilişim suçunun aydınlatılması için veri

toplama, silinen ve değiştirilen verilerin kurtarılmasını sağlama, bu delillerin hukuki ve etik çerçevede analiz edilerek yorumlanması ve belgelenmesini sağlayan tüm süreçleri içerir (İnternet, Barry). Bilgi güvenliğinin alt dalından biri olan adli bilişim doğası gereği bilgisayar ve hukuk bilimlerinin bir sentezi olarak ortaya çıkan bilim dalıdır (Sağiroğlu ve Karaman, 2012). Adli bilişim sayesinde bilişim suçunu işlenme biçimi ortaya koyulmakta ve adli makamlarca suçu işleyen kişi/kişiler yargılanarak cezalandırılabilir (Başlar, 2019). Bu durum, bilişim suçu işleme potansiyeli olan kişi veya kişiler için caydırıcı bir unsur olabilmektedir. Adli bilişim sadece işlenen suçun analizi ve hukuka delil sağlanmasına yardımcı olmaz. Ayrıca işlenen suçun nasıl ve ne şekilde yapıldığını araştırarak mevcut sistem açıklarının gelişen teknoloji karşısında nasıl bir korunma mekanizması oluşturacağını da yardımcı olmuş olur. Adli bilişim, siber uzayda yapılan saldırılar sonucunda bilgi güvenliği için yürütülen çalışmaları kapsamaktadır (Varol, Cooper ve Varol, 2013). Bu nedenle, adli bilişim aynı zamanda bilgi güvenliği ve hukukun birleştiricisi görevini üstlenmektedir (Dlamini, Eloff ve Eloff, 2009). Sonuçta, yaşanan önemli bir bilgi güvenliği ihlali sonrası olayın aydınlatılmasını sağlayacak en büyük yardımcı adli bilişim incelemesi olacaktır (Rowlingson, 2004). Adli bilişim; bilgi güvenliğinin sağlanmasına yardımcı olarak yürütülebilecek farkındalık faaliyetlerinin bir parçasını oluşturabilir. Çünkü adli bilişim, bilgi güvenliği alanını anlamlandırma ve bu alan için farkındalık oluşturmaya yardım etmektedir (Whitman ve Mattord, 2021).

Adli bilişimin, işlenen bilişim suçunu tespit etme ve analiz etme yeteneği sayesinde; bilgi güvenliğinin sağlanması ve bilgi güvenliği farkındalığının oluşması için yardımcı olabilmektedir. Adli bilişim alanının, kişilerce bilinmesi bu konu hakkında farkındalık eğitimlerinin belirlenerek sektöre uzman yetiştirilmesi de diğer önemli hususlardan biridir. Sonuçta adli bilişim mühendisliği eğitimi bilişim suçları ile mücadele eden hem kamu kurumları hem de özel sektöre yönelik uzman kişi yetiştirerek bu alanki farkındalığı arttırmaktadır (Akbal ve Güneş, 2016). Bilgi güvenliğinin alt çalışma prensiplerinden biri olan adli bilişim konusunda farkındalık çalışmalarının yürütülmesi bilgi güvenliği farkındalığının oluşmasına yardımcı olabilecektir. Ülkemizde adli bilişim kavramının 2006 yılından itibaren bilinirliğinin artarak devam etme eğilimi göstermiştir (Karakuş, 2018). Ülkemizde, adli bilişim alanında uzman yetiştirmek için gerek kamu gerek akademik olarak eğitimler verilmektedir (Varol, Cooper ve Varol, 2013) SANS Enstitü tarafından verilen Küresel Bilgi Güvencesi Sertifikasyon (GIAC-Global Information Assurance Certification) çalışmasında; bilgi güvenliği hakkında uzman olmak isteyen çalışanlara adli bilişim ve olay

müdahalesi, yazılım güvenliği, hukuk ve güvenlik uzmanlığı ile daha birçok güvenlik konusunu kapsayan eğitimler verilmektedir (İnternet, GIAC). Kişilerin bilgi güvenliği uzmanlığını kazanabilmeleri için bilişim suçlarının nasıl ve hangi yöntemler işlenerek sağlandığını bilmeleri işlenen suçun doğru analiz edilmesi açısından önemlidir. Yavuz ve Ulaş'ın (2013) çalışmasında, bilgi güvenliği, bilişim suçları ve adli bilişim hakkında kişilere sorular sorularak fikirleri alınmıştır. Bu çalışma sonucunda, kişilerin işlenen bilişim suçlarını yeterince bilmediği, bu konuda işlenen suçların hukuki yaptırımının yetersiz olduğu ve bazılarının işlenen suç nereye bildireceğini bile bilmedikleri ifade edilmiştir. Ayrıca katılımcıların büyük çoğunluğu, Türkiye'de adli bilişimin gelişmesi için hem kamu kurumları hem de özel sektöre yönelik konu hakkında farkındalık çalışmalarının yürütülmesi gerektiğini belirtmiştir. Bostan ve Akman'ın (2011) çalışmasında, katılımcıların web güvenliği konusundaki eğitim ve deneyim düzeylerindeki artışın bu konu hakkındaki farkındalıklarını arttırdığı belirtilmiştir. Dijle ve Doğan'a (2011) göre; bilişim suçunun oluşmadan önlenmesi için önceden tedbir alınması gerektiği ve konu hakkında farkındalık faaliyetlerinin yürütülmesi gerektiği belirtilmiştir. Gerek adli bilişim gerek bilgi güvenliği farkındalığının gelişmesi; işlenen veya işlenecek olan bilişim suçu yöntemlerinin bilinmesine, bu saldırılara karşı geliştirilecek güçlü savunma stratejisine ve bu konu hakkında farkındalığı yüksek bireylere bağlıdır. Bilgi güvenliği ve adli bilişim hakkında farkındalık düzeyi yüksek bireyler; kişisel, kurumsal ve ulusal bilgi güvenliğine katkı sağlayacaktır. Sonuçta kişiler her gün hem bireysel hayatlarında hem de kamu ve özel sektör ayırt etmeksizin çalıştıkları kurumlarda siber saldırıya maruz kalabilmektedir. Bu durumda yaşanan veya yaşanması muhtemel bilişim suçunun fark edilebilmesi için konu hakkında tüm çalışanların farkında olması ve suçu yetkililere bildirmeleri oldukça önemlidir. İşlenen bilişim suçunun bildirildikten sonra etik kurallar çerçevesinde adli bilişim kurallarınca analiz edilmesi ve hukuksal sürecin başlatılması bilgi güvenliğini sağlamak için önemli bir adımdır (Henkoğlu, 2020). Bilişim suçu karşısında doğru adli analizin yapılması olayların aydınlatılmasını sağlayacaktır (Akbal, Doğan, Tuncer ve Atalay, 2019) Kurumsal bilgi güvenliği farkındalığı ve adli bilişim ilişkisini sadece bununla sınırlandırılmamalıdır. Bilişim suçları ve işleme yöntemlerinin adli bilişim/siber güvenlik uzmanlarınca çeşitli farkındalık faaliyetleri ile kurum çalışanlarına aktarmaları da bu sürecin bir parçası olmalıdır (Özdemir, Kalkan, Türkoğlu, Varol ve Tokdemir, 2013). Sonuçta; kurumsal bilgi güvenliği farkındalık faaliyetlerinin içeriği sadece; bilgi güvenliği ve ilgili kavramlar, bilgi güvenliği sağlama yöntemleri gibi konular değildir. Kurumsal bilgi güvenliği farkındalık faaliyetlerine; daha önce yaşanan bilişim suçları ve yöntemleri, kişilerin bir bilişim suçuna

maruz kaldığında yapması gerekenler gibi konu başlıkları dâhil edilmeli ve yürütülen bu faaliyetlerinde konunun daha iyi anlaşılması için gerçek olay örneklemeleri adli bilişim uzmanlarınca aktarılmalıdır.

3.3. Kurumsal Bilgi Güvenliği Farkındalığı ile İlgili Yapılan Alanyazın Çalışmaları

Kurumsal bilgi güvenliği farkındalığı hakkında alanyazında gerek ulusal gerek uluslararası tez, makale, bildiri gibi birçok çalışma mevcuttur. Bu çalışmalar sayesinde kurumsal olarak bilgi güvenliği farkındalığı farklı boyutları ile ele alınmış ve kendini geliştirme imkânı bulmuştur. Yapılan çalışmalarda kurumsal bilgi farkındalığı veri toplama aracı olan ölçek ve anket çalışmaları ile sağlanmıştır ve belirli bir hedef kitle seçilip bu kitlenin farkındalık düzeyi ölçümlenmiştir. Hedef kitle, kimi zaman kamu kurumunda çalışan kişiler olurken kimi zamanda belirli bir alanda çalışan özel sektör çalışanlarına yönelik yapıldığı gözlemlenmiştir. Bazen de hedef kitle, bir il veya belirli bir pozisyonda çalışan kişilere yönelik oluşturulmuştur. Meslek grupları ile yapılan çalışmalarda ise bilgi güvenliği farkındalığını ölçmek için hedef kitle seçilen meslek grubunun diğer meslek grupları ile karşılaştırılması yapılmıştır. Alanyazında incelenen çalışmalarda dikkate alınan önemli husus; bireysel bilgi güvenliği farkındalığından ziyade kurumsal bilgi güvenliği farkındalığı üzerine yapılan çalışmaların incelenmesine yöneliktir.

Özdemir ve Uluyol (2021) tarafından yapılan çalışmada; kamu kurumunda çalışan beş yüz bir kişiye yönelik ölçek uygulanmıştır. Çıkan sonuçta, alınan puanların ortalamasına göre katılımcıların orta seviye bilgi güvenliği farkındalığına sahip oldukları sonucuna varılmıştır. Cinsiyete göre kadın ve erkeklerin yakın seviye bilgi güvenliği farkındalık düzeyine sahip oldukları gözlemlenirken 40 yaş altı ile teknik eğitim alan bilgi teknolojik çalışanlarının bilgi güvenliği farkındalık düzeyleri yüksek çıkmıştır. Çalışma sonundaki öneri, bilgi güvenliği farkındalık düzeyini arttırmak için verilen eğitimlerin dinamizmini koruyarak güncel tutulması ve sürdürülebilir olmasının hedeflenmesi şeklinde ifade edilmiştir.

Köktürk ve Avcı (2019) tarafından yapılan çalışmada; kamu kurumunda çalışan yetmiş iki kişiye yönelik ölçek uygulanmıştır. Toplanan verilerin analizinde frekans ve yüzde dağılımları esas alınmıştır. Katılımcıların bilgi güvenlik farkındalık düzeyleri yüksek olduğu görülmüştür. Ölçek çalışmasına katılan kişilerin en az güvenlik duvarı yazılımı konusunda en fazla da parolaların herhangi bir ortamda saklanmasının güvenlik riski oluşturacağı konusunda farkında oldukları belirtilmiştir. Çalışma sonundaki öneri, kurum çalışanlarına

bilgi güvenliği farkındalığı üzerine eğitim verilmesinin faydalı olacağı yönünde ifade edilmiştir.

Çakır ve Tuygun (2019) tarafından yapılan çalışmada; ISO 27001: BGYS sertifika sürecini tamamlamış kamu kurumlarındaki 539 kurum personeline anket uygulanmıştır. Çıkan sonuçların analizi yapılırken grupların frekans ve yüzde dağılımları esas alınmıştır. Yönetim kadrosu, ISO 27001 sertifikasyon süreci olumlu karşılarken BGYS ekip üyeleri ISO 27001 sürecinde teknik yeterlilik, eğitim gibi destek ihtiyaçları olduğunu belirtmiştir. Teknik personel, ISO 27001 süreçlerinin işlerini kolaylaştırdığını belirtirken; kurum personeli ISO 27001 farkındalık eğitimlerini faydalı bulmuş ve BGYS süreçlerinin kurumun bilgi güvenliği için olması gerektiği yönünde görüş bildirmişlerdir. Çalışma sonundaki öneri, kurumsal BGYS ve ISO 27001 belgesi için kurum sisteminin sürekliliği esas alınmalı ve konu hakkındaki farkındalık eğitimlerinin mutlaka olması gerektiği ifade edilmiştir.

Ceylan (2019) tarafından yapılan çalışmada; iki yüz bilişim çalışanına ölçek uygulamıştır. Verilerin analizi için t-testi ve tek yönlü Anova testi kullanılmıştır. Çalışmaya katılanların bilgi güvenlik farkındalık seviyeleri yüksek çıkmıştır. Çıkan sonuca göre; ileride katılımcı sayısı artırılarak bir farkındalık analiz çalışması yapılacağı belirtilmiştir.

Okul ve diğerleri (2018) tarafından yapılan çalışmada; Kuşadası'nda yer alan beş yıldızlı konaklama işletmelerinde bulunan elli iki yöneticiye ölçek uygulamıştır. Yöneticilerin anket sorularına verdikleri cevapların ortalamaları çıkarılmış ve bunlara t testi ve tek yönlü Anova testi uygulanmıştır. Çıkan sonuçlara göre; yöneticilerin bilgi güvenliği farkındalık seviyeleri yüksek çıkmasına rağmen bilgi güvenliği konusunda bazı önemli noktalarda bilgi sahibi olmadıkları belirtilmiştir. Çalışma sonundaki öneri, konaklama işletmelerine yönelik bilgi güvenliği eğitimlerinin verilme gerektiği ifade edilmiştir.

Yılmaz, Şahin ve Akbulut (2015) tarafından yapılan çalışmada; “dijital veri güvenliği farkındalık ölçeği” geliştirmek için yetmiş dokuz öğretmen ile ölçek formu ön deneme uygulamasını gerçekleştirmiştir. Bu uygulama sayesinde başka meslek grupları ve başka çalışmalar da dâhil olmak üzere alanyazına bir ölçek kazandırılmıştır. Geliştirilen ölçek neticesinde çıkan sonuç; dijital veri güvenliği hakkında olması muhtemel tehdit ve sorunlar karşısında insan faktörünün bilinçlendirilmesi gerektiğidir. Bu ölçek çalışması hem uygulama alanındaki genişliği hem de bu alandaki ölçek çalışmalarının çeşitliliğini arttırmıştır.

Öztemiz ve Yılmaz (2013), tarafından yapılan çalışmada; Ankara ilinde bulunan on dört kütüphanedeki kütüphane ve dokümantasyon daire başkanları veya yardımcıları ile doğrudan ya da telefonla görüşüp nitel yöntem kullanarak bilgi güvenliği farkındalığı hakkında veri toplanmıştır. Araştırma sonuçlarına göre kütüphanelerin büyük kısmı bilgi güvenliğinin sağlanması gerektiğini belirtirken bilgi güvenliği hakkında olan uygulamaların içeriğinin yeterince bilinmediği ve uygulamaların bilgi işlem daire başkanlarınca yürütüldüğü sonucuna varılmıştır. Çalışma sonundaki öneri; kütüphanelerde bilgi güvenliğinin sağlanması için çalışanlara farkındalık eğitimleri ile beraber görev ve sorumluluk bilincinin aşılması gerektiği ifade edilmiştir.

Mart (2012) tarafından yapılan çalışmada; 2010-2012 yılları arasında farklı illerde ve farklı meslek gruplarında çalışan beş yüz bir kişiye anket uygulanmıştır. Toplanan verilerin analizi için t testi ve tek yönlü Anova testi kullanılmıştır. Katılımcıların yaş gurubu ve bilgisayar kullanımının süresi arasında anlamsal bir fark olmuştur. Çalışma sonundaki öneri; bilgi güvenliği farkındalığı hakkında küçük yaşlardan itibaren eğitim verilmesi gerektiği şeklinde ifade edilmiştir.

Erol, Ceyhan ve Sağıroğlu tarafından yapılan çalışmada; bireysel, kurumsal ve ulusal bilgi güvenliği farkındalığı ortaya koymak için bu üç kategorinin de en önemli unsurunun insan olduğunu ifade ederek insana yatırım yapılması gerektiğinin altını çizmiştir. Ayrıca bilgi güvenliği farkındalığının nasıl bir yaşam döngüsü olduğu şekillendirilerek kavramın daha rahat anlaşılması sağlanmıştır. Bununla beraber bilgi güvenliğini tehdit eden durumlar için ulusal ve uluslararası yaşanmış olaylar ifade edilerek çalışma sonunda bilgi güvenliği farkındalığının önemi vurgulanmıştır.

Çelikçöp ve Yazar (2019) tarafından yapılan çalışmada; İstanbul ilinde bulunan Kamu Hastaneler Birliğine bağlı yetmiş iki kamu hastanesinin kalite yönetim direktör ve kalite birim sorumlularına ölçek uygulanmıştır. Katılımcıların cevapları; frekans yüzde, ortalama, standart sapma, t-testi ve Anova testi kullanılarak analiz edilmiştir. Ölçek; “saldırı ve tehditler” ile “kişisel verilerin korunması” olmak üzere iki alt boyuttan oluşan 5’li Likert tipindedir. Çıkan sonuçlara göre; katılımcıların “kişisel verilerin korunması” düzeyi yüksek, “saldırı ve tehditlere yönelik farkındalık” düzeyi orta ve genel “bilgi güvenliği farkındalığı” düzeyinin orta seviyede olduğu belirtilmiştir. Çalışma sonundaki öneri, bilgi güvenliğinin sağlanabilmesi için teknolojiden ziyade insan faktörü ele alınmalı ve yöneticilerde dâhil olmak üzere tüm personelin bu sürece katkı sağlamalı gerektiği şeklinde ifade edilmiştir.

Kjørvik (2010) tarafından yapılan çalışmada; öğrencilere anket uygulanmıştır. Anketin başarılı olması için ön anket hazırlanmış ve buradaki hatalara bakılarak ana anket düzenlenmiştir. Çalışmanın temel amacı; güvenlik farkındalığı hakkında mevcut ifadeleri tartışarak olası yöntemleri karşılaştırmaktır. Çalışma sonundaki öneri, bilgi güvenliği farkındalığı için uygulanan yöntemlerin tartışılarak veya ön elemenden geçirilerek iyileşmesini sağlaması gerektiği şeklinde ifade edilmiştir.

Veseli (2011) tarafından yapılan çalışmada; katılımcılara bilgi güvenliği farkındalığı eğitimi verilmeden önce ve verildikten sonra hazırladığı çevrimiçi anketi uygulanmıştır. Katılımcıların cevapları; t-testi ve Anova testi kullanılarak analiz edilmiştir. Çalışmada sınıf eğitimi, tartışmaya dayalı eğitim ve web tabanlı eğitim stillerinde farkındalık eğitimleri verilmiştir. Sınıf eğitiminin; tartışmaya dayalı ve web tabanlı eğitime göre daha etkili olduğu sonucuna ulaşılmıştır. Çalışmanın temel amacı; insan faktörünün bilgi güvenliği konusunda aldığı eğitime göre farkındalık seviyesinin nasıl değiştiğini ölçümlemektir. Çalışma aynı zamanda alınan eğitimin farklı stillerde olmasında farkındalık düzeyine olan katkısını ortaya koymaktadır. Çalışma sonundaki öneri; etkili bilgi güvenliği için insan faktörü daima göz önünde bulundurulmalı ve bilgi güvenliği konusunda verimli eğitim stili ile insanın farkındalık düzeyi artırılması gerektiği ifade edilmiştir.

Kruger, Drevin ve Steyn (2010) tarafından yapılan çalışmada; bir üniversitedeki iki farklı öğrenci grubuna bilgi güvenliği farkındalık düzeyini anlamak için kelime testi ve davranış değerlendirme bölümlerinden oluşan anket çalışması uygulanmıştır. Bu anketle amaçlanan; katılımcıların bilgi güvenliği kavramları hakkında sahip olduğu bilgi düzeyini ölçerek kurumsal bilgi güvenliği farkındalık programlarına yeni bir uygulama kazandırmaktır. Çalışma sonucundaki öneri, kelime testinin faydalı bulunduğu ve bilgi güvenliği farkındalık düzeyinin belirlenmesinde yardımcı olacağı şeklinde ifade edilmiştir.

Kruger ve Kearney (2006) tarafından yapılan çalışmada; uluslararası bir maden şirketi için bilgi güvenliği farkındalığı konusunda prototip geliştirmiştir. Otuz beş sorudan oluşan ölçek çalışmasındaki puanlamada; 100-80 arası “iyi”, 79-60 arası “orta” ve 59 altı “düşük” olarak sınıflandırılmıştır. Alınan ortalama puana göre şirket çalışanlarının bilgi güvenliği genel farkındalığı % 65 ölçülerek orta derecede kabul edilmiştir. Çalışma sonucundaki öneri, bu prototipin hayata geçirilmesi için ölçümlemenin bölgesel düzeylerden genel bir ölçümleme düzeyine taşınması gerektiği ifade edilmiştir.

Hadlington ve Chivers (2020) tarafından yapılan çalışmada; 18 ile 84 yaş arasında bin elli dört kişinin katılım gösterdiği, siber suç duyarlılığının bilgi güvenliği farkındalığı ve kişilik faktörü arasındaki ilişkiye etkisi üzerine ölçek uygulanmıştır. Ölçek, 26 sorudan oluşan 11'li Likert tipinde hazırlanmıştır. Çıkan sonuca göre; katılımcıların % 60 siber suça yatkınlık konusunda yüksek risk kategorisinde yer almakla birlikte bilgi güvenliği farkındalığında düşük ancak dürtüsellik konusunda yüksek düzeyde yer almışlardır. Çalışma sonucundaki öneri, siber suça karşı oluşan hassasiyetin anlaşılması için ele alınan segmentasyon farkındalık düzeyinin kapsamının genişletilmesi gerektiği ifade edilmiştir.

Kaur ve Mustafa (2013) tarafından yapılan çalışmada; Malezya'daki bir Küçük ve Orta Büyüklükteki İşletme'nin (KOBİ) 110 çalışanının katıldığı bilgi güvenliği farkındalığı ölçeği uygulanmıştır. Bu ölçek çalışmada, katılımcıların; gizlilik, bütünlük ve kullana bilirlik ilkeleri hakkındaki tutumları ölçümlenmek istenmiştir. Çalışmanın temel amacı, KOBİ çalışanlarının bilgi güvenliği farkındalık düzeyini ölçmektir. Çalışma sonuçlarına göre; çalışanların işyerindeki bilgi kaynakların gizliliği konusunda farkındalık düzeyleri yüksektir. Ancak çalışanların kimlik avı içeren e-postalar hakkında farkındalık düzeyleri düşüktür. Bu nedenle çalışma sonundaki öneri, ölçeğe katılan kişilere bu yönde eğitim verilmesi gerektiği ifade edilmiştir.

Yukarıdaki çalışmalar incelendiğinde, bilgi güvenliği farkındalığı hakkında daha çok yaş, cinsiyet, farklı meslek grupları gibi değişkenlere odaklanılarak seçilen gruptaki çalışanlar aynı işyerlerine mensuptur. Yapılan bu çalışma ise daha önce yapılan çalışmalara katkı sağlamak için farklı sektör çalışanlarının bilgi güvenliği farkındalık seviyesini cinsiyet, yaş, çalışılan kurum türü, pozisyon gibi değişkenlere göre değişiklik gösterip göstermediği konusunda inceleme sağlayarak iki sektör çalışanlarını bilgi güvenliği farkındalığı hakkında kıyaslama olanağı verebilecektir. Kısaca bu araştırma, hem farklı sektör çalışanlarının bilgi güvenliği farkındalık düzeyini ölçümlemek hem de sektör farklılığının çalışanlar arasında bilgi güvenliği farkındalığına anlamlı bir katkısı olup olmadığını kıyaslayarak analiz etme imkânı sunacaktır.

4. YÖNTEM

Bu bölümde yapılan araştırmada kullanılan yöntem açıklanmıştır. Ayrıca araştırma modeli başta olmak üzere araştırma, çalışma grubu, veri toplama süreci ve aracı ile veri analizine yer verilmiştir.

Araştırma modeli

Belirlenen kamu kurumu ve özel sektör çalışma grubunda bilgi güvenliği farkındalık düzeyini ortaya koymak üzere araştırma için tarama modeli kullanılmıştır. Tarama modelleri, bir olay veya durumu olduğu gibi betimlemeyi amaçlayan modellerdir (Karasar, 2020, s. 109). Bu modelin kullanılmasındaki amaç; durumun halen var olması ve betimlenmeye ihtiyaç duymasından dolayıdır. Bu model, araştırmadaki birey ve nesneyi tanımlarken olayları değiştirmez (Karasar, 2012, s. 80)

Araştırmanın çalışma grubu

Araştırmanın çalışma grubunu; 2021 yılında Ankara ilinde bilişim sektörü alanında çalışan toplam 138 kamu kurumu ve özel sektör çalışanı oluşturmaktadır. Araştırmaya katılan çalışanlar ile ilgili demografik özelliklere Çizelge 4.1’de yer verilmiştir.

Çizelge 4.1. Araştırmaya katılan çalışanlar hakkındaki demografik özellikler

Sorular		n	%	Toplam
Cinsiyet	Kadın	33	23,9	138
	Erkek	105	76,1	
Kurum türü	Kamu kurumu	85	61,6	138
	Özel sektör	53	38,4	
Yaş	20-29 yaş arası	50	36,2	138
	30-39 yaş arası	60	43,5	
	40-49 yaş arası	23	16,7	
	50 ve üzeri	5	3,6	
Öğrenim durumu	Lise	1	0,7	138
	Ön Lisans	11	8	
	Lisans	75	54,3	
	Yüksek Lisans	46	33,4	
	Doktora	5	3,6	
Çalışılan pozisyon	Yönetici	22	15,9	138
	Teknik personel	81	58,7	
	İdari personel	35	25,4	
Bilgi güvenliği farkındalığı hakkında işyerinde eğitim/kurs veriliyor mu?	Evet	121	87,7	138
	Hayır	17	12,3	
Bilgi güvenliği farkındalığı üzerine işyerinde ne sıklıkla eğitim/kurs veriliyor?	Üç ayda bir	20	16,5	121
	Altı ayda bir	58	47,9	
	Yılda bir	28	23,2	
	Bir yıldan fazla	15	12,4	
İşyerinde verilen bilgi güvenliği farkındalığı eğitimleri/kursları ne kadar faydalı?	Çok faydalı	41	33,9	121
	Faydalı	65	53,7	
	Karasızım	10	8,3	
	Faydasız	5	4,1	
İşyerinizde bilgi güvenliği politikası mevcut mu?	Evet	132	95,7	138
	Hayır	6	4,3	
İşyerinizde bilgi güvenliği politikasının uygulanma derecesi nedir?	Oldukça uygulanıyor	69	50	138
	Uygulanıyor	52	37,7	
	Uygulanmıyor	4	2,9	
	Hiç uygulanmıyor	1	0,7	

(f: frekans, %: yüzde)

Çizelge 4.1'e göre katılımcıların 33'ü kadın (% 23,9) ve 105'i erkektir (% 76,1). Bu iki katılımcı oranı kıyaslandığında erkek katılımcılar kadın katılımcılardan üstün bir çoğunlukla fazladır. Bu durumun nedeni; Türkiye'deki istihdam edilen kadın oranının (% 26,3) erkek oranına (% 59,8) göre yarısından daha az olmasıdır (TÜİK, 2021). Başka bir neden ise; kadınların bilgi teknoloji sektöründeki çalışma oranlarının düşük olmasıdır. Bilişim Sanayicileri Derneğinin (TÜBİSAD) 2018 yılında yayınladığı "*Teknoloji Sektöründe Kadın Raporuna* göre Türkiye'de bilgi teknoloji sektöründe çalışan kadın oranı %7'dir (TÜBİSAD, 2018). 2018 yılında Honeypot tarafından aralarında Türkiye'nin de bulunduğu 41 ülkeyi kapsayan *2018 Teknoloji Kadınlar Endeksi* araştırmasında 2018 yılında Türkiye'nin teknoloji endüstrisinde çalışan kadın sayısının oranının % 9,91 olduğu belirtilmiştir (Honeypot, 2018). Kadınların erkeklere göre hem istihdam edilme oranındaki düşüklük hem de bilgi teknolojide daha az yer almaları çalışmanın cinsiyet katılımındaki oransal farklılığı oluşturmuştur. Katılımcıların çalıştıkları kurum türüne göre; 85'i kamu kurumu (% 61,6) ve 53'ü özel sektörde (% 38,4) çalışmaktadır. Katılımcıların çoğunluğu 30-39 yaş grubunda (% 43,5) toplanmıştır, bu yaş grubunu 20-29 yaş grubu (% 36,2) ve 40-49 yaş grubu (% 16,7) takip etmektedir. Katılımcıların yarısından fazlası *lisans* mezunu (% 54,3) olup bu öğrenim durumunu *yüksek lisans* (% 33,4) ve *ön lisans* (% 8) mezunu katılımcılar takip etmektedir. Katılımcıların işyerinde çalıştıkları pozisyona göre, çoğunluğu (% 58,7) *teknik personel* oluşturmakta ve bu oranı *idari personel* (% 25,4) ile *yönetici* (% 15,9) kadrosunda çalışan kişiler takip etmektedir.

Bilgi güvenliği farkındalığı hakkında çalıştıkları işyerinde eğitim/kurs verilmesi durumu hakkında katılımcıların büyük çoğunluğu *evet* (% 87,7) cevabı verirken geriye kalan katılımcılar *hayır* (% 12,3) cevabı vermiştir. Bilgi güvenliği farkındalığı hakkındaki eğitimlerin/kursların ne sıklıkla verildiği sorusuna *evet* cevabı veren 121 kişinin çoğunluğu *altı ayda bir* (% 47,9) seçeneğini tercih ederken bu seçeneği *yılda bir* (% 23,2) ve *üç ayda bir* (% 16,5) seçenekleri takip etmektedir. Alınan bu eğitimin faydası konusunda yine *evet* cevabı veren 121 kişinin çoğunluğu eğitimi *faydalı* (% 53,7) bulurken bu seçeneği *çok faydalı* (% 33,9) ve *kararsızım* (% 8,3) seçenekleri takip etmektedir. Çalışılan firmada bilgi güvenliği politikasının mevcut olma durumu konusunda büyük çoğunluk *evet* (% 95,7) cevabı verirken diğer katılımcılar *hayır* (% 4,3) cevabı vermiştir. Bunlara ek olarak işyerlerinde bilgi güvenliği politikasının uygulanma derecesine ise katılımcıların yarısı *oldukça uygulanıyor* (% 50) seçeneğini tercih ederken, bu oranı *uygulanıyor* (% 37,7) ve *kararsızım* (% 8,7) seçenekleri takip etmektedir.

Veri toplama süreci

Verilerin toplanma sürecinde ilk olarak Gazi Üniversitesi Etik Komisyonuna başvurularak gerekli izinler alınmıştır. Etik komisyondan alınan izni takiben uygulanacak veri toplama aracı, insan kaynakları birimi tarafından kamu ve özel sektör çalışanlarının kurumsal e-postasına iletilmiştir. Bu çalışmaya katılmadan önce kişilere gönüllülük esası ile çalışmaya katılacakları ve istedikleri zaman çalışmadan ayrılacakları bununla beraber toplanan verilerin sadece bilimsel amaçla kullanılacağı konusunda gerekli bilgilendirilme sağlanmıştır. Bu çalışmaya 138 kişi katılım sağlamıştır.

Veri toplama aracı

Araştırma için veri toplama aracı olarak Çatuk (2018) tarafından geliştirilen açımlayıcı ve doğrulayıcı faktör analizi yapılan 37 madde oluşan ölçek kullanılmıştır. 5'li Likert tipinde hazırlanan bu ölçekte katılımcılardan 1=Kesinlikle katılmıyorum, 2=Katılmıyorum, 3=Kararsızım, 4=Katılıyorum, 5=Kesinlikle katılıyorum şıklarından uygun buldukları seçeneği tercih etmeleri istenmiştir. Bu çalışmada Cronbach's Alpha iç tutarlılık katsayısı (α) .96 olarak hesaplanmıştır. Çatuk tarafından hesaplanan Cronbach's Alpha iç tutarlılık katsayısı .954'tür. Ölçek, "Gizlilik", "Bütünlük", "Mahremiyet", "Erişilebilirlik" olmak üzere 4 faktörden oluşmaktadır. Çalışma için elde edilen toplam varyans % 67,33'tür ve "Gizlilik" faktörü varyans oranının % 42,17'sini, "Bütünlük" faktörü % 10,16'sını, "Mahremiyet" faktörü % 8,56'sını ve "Erişilebilirlik" faktörü de % 6,44'ünü oluşturmaktadır (Çatuk, 2018).

Veri analizi

Bu çalışma için toplanan verilerin analizi, istatistiksel analiz programı olan SPSS 25'te yapılmıştır. Analizler yapılırken ölçüm puan ortalaması alınarak hesaplanmıştır ve soruların kapsamına göre betimsel istatistik kullanılmıştır. Betimsel istatistik, toplanan verilerin analiz edilmesi ile beraber yorumlanıp özetlenmesini ifade eder (Özsoy, 2014, 4). Çalışmada madde-toplam korelasyon katsayısı 0,40'dan küçük olan 2, 14, 17 ve 18. sorular analizden çıkarılmıştır. Ölçek güvenilirliği, kişilerin ölçek maddelerine verdikleri cevaplar arasındaki tutarlılık biçimiyle ifade edilebilir (Büyüköztürk, 2002, 181). Cronbach's Alpha katsayısı, yapılan çalışmanın güvenilirliğini belirleyen bir tekniktir (Gliem ve Gliem, 2003, 83) ve iç tutarlılığı değerlendirmek için yararlı bir katsayıdır (Bland ve Altman, 1997, 572). Bu çalışmada, toplanan verilerin güvenilirlik analizi sonucunda Cronbach's Alpha iç tutarlılık

katsayısı (α) .96 ve ölçek % 96 oranında güvenilirdir. Bu katsayı .80 ile 1 değeri arasındaysa yapılan ölçeğin güvenilirliği *yüksek güvenilirliktedir* (Uzunsakal ve Yıldız, 2018, 19). Bu ölçek çalışması da yüksek güvenilirliktedir.

Normalliğin sınanması

Verilerin dağılımını anlamak için normalliğin sınanması, normallik testlerinin uygulandıktan sonra öğrenilmektedir (Ballı ve Önder, 2019, 519). Normalliğin sınanması, ölçüm ortalamasına çarpıklık-basıklık ve Kolmogrov-Smirnov testi uygulanarak gerçekleştirilmiştir (Varlı ve Uluçınar Sağır, 2019). Çizelge 4.2’de ölçüme ait çarpıklık, basıklık ve Kolmogrov-Smirnov sonucunda ortaya çıkan p değerine yer verilmiştir.

Çizelge 4.2. Normalliğin Sınanması

	Çarpıklık	Basıklık	p
Bilgi güvenliği farkındalığı ölçeği	-1,859	3,475	0,000

(p: anlamlılık düzeyi)

Alanyazında normalliğin sınanması için çarpıklık ve basıklık değer aralıkları farklılık gösterebilmektedir. Bazı çalışmalarda, verilerin normal dağılıma sahip olabilmesi için çarpıklık ve basıklık değerlerinin -1 ile +1 aralığında olması gerektiği belirtilmiştir (Huck, 2012, George ve Mallery, 2019). Bazı çalışmalarda ise -1,5 ile +1,5 aralığında olması gerektiği belirtilmiştir (Tabachnick, Fidell ve Ullman, 2007, s. 67) Diğer görüşlere göre; ölçüm için elde edilen çarpıklık ve basıklık -2 ile +2 (Sevgi ve Yakışıklı, 2020, s. 406) değer aralığında veya -3 ile +3 (Jondeau ve Rockinger, 2003, s. 1719) değer aralığında olması da verilerin normal dağıldığının bir göstergesi olarak kabul edilir. Çizelge 3.2’ye göre çarpıklık ve basıklık değer aralığının, alanyazında belirtilen çarpıklık ve basıklık değer aralığının dışında olduğu görülmektedir.

Normalliğin sınanması için bakılacak diğer değer de Kolmogrov-Smirnov testinin sonucunda ortaya çıkan p değeridir. $p < 0,05$ ise veriler normal dağılmamaktadır. Eğer $p > 0,05$ ise veriler normal dağılmaktadır (Büyüköztürk, 2010, s. 70). Alanyazındaki bu değerlendirme sonucunda p değerinin 0,05’den küçük olduğu Çizelge 3.2’de görülmektedir. Bunun sonucunda çarpıklık ve basıklık değerlerinde olduğu gibi Kolmogrov-Smirnov testi sonucunda oluşan p değeri için de verilerin normal dağılım göstermediği görülmektedir.

Veriler normal dağılım göstermediği için Mann-Whitney U ve Kruskal-Wallis H istatistiksel testleri uygulanmıştır. (Demirel, Işık, Demirel, Üstün ve Gümüşgöl, 2016). Bu testler sonucu elde edilen değerler çizelge haline getirilerek istatistiksel olarak yorumlanmıştır.



5. ARAŞTIRMA BULGULARI

Yapılan çalışmada verilerin normal dağılmadığına karar verilerek uygulanan Mann-Whitney U ve Kruskal-Wallis H istatistiksel testleri sonucunda elde edilen bulgular ile çalışmaya katılan kişilerin bilgi güvenliği farkındalık düzeylerinin dağılımı aşağıda verilmiştir.

Bu çalışmanın belirleyici sorulardan kurum türünün bilgi güvenliği farkındalığı üzerine etkisinin Mann Whitney U testi sonucu Çizelge 5.1’de görülmektedir.

Çizelge 5.1. Bilgi güvenliği farkındalığının kurum türüne göre Mann Whitney U testi sonucu

Kurum Türü	n	Sıra Ortalaması	Sıra Toplamı	U	p
Kamu kurumu	85	67,11	5704,5	2049,5	0,373
Özel sektör	53	73,33	3886,5		

Çizelge 5.1 incelendiğinde özel sektör sıra ortalamasının kamu kurumu sıra ortalamasına göre daha yüksek olduğu görülmekle beraber bu fark istatistiksel olarak anlamlı değildir. Bilgi güvenliği farkındalığında, kurum türüne göre anlamlı düzeyde farklılaşma olmadığı görülmektedir ($p>0,05$). Bu sonuca göre, “*H1: Özel sektör çalışanlarının bilgi güvenliği farkındalığı kamu kurumu çalışanlarına göre daha yüksektir.*” hipotezi reddedilmiştir.

Çalışmadaki katılımcıların bilgi güvenliği farkındalığında ölçeğindeki yanıtların 1,24 ile 4,88 arasında değişmektedir. Ölçeğin ortalaması 4,11 ve standart sapması 0,785 olarak bulunmuştur. Sonuçlar Çizelge 5.2’de görülmektedir.

Çizelge 5.2. Bilgi güvenliği farkındalığı ölçeği ve ortalaması

	n	Ortalama	St. Sapma	Minimum	Maksimum
BGF Ölçeği	138	4,1192	0,7855	1,24	4,88

(n: gözlem/kşi sayısı, st. Sapma: standart sapma)

Ölçek ortalamasının en üst değer olan 4,88’e oldukça yakın olduğu görülmekle beraber bu sonuca göre, “*H2: Bilişim çalışanlarının bilgi güvenliği farkındalığı diğer çalışanlara göre daha yüksektir.*” hipotezi kabul edilmiştir. Kısaca, çalışmaya katılan kişilerin bilgi güvenliği farkındalık düzeyi yüksektir.

Bilgi güvenliği farkındalığının cinsiyete göre Mann Whitney U testi sonucu Çizelge 5.3’te görülmektedir.

Çizelge 5.3. Bilgi güvenliği farkındalığının cinsiyete göre Mann Whitney U testi sonucu

Cinsiyet	n	Sıra Ortalaması	Sıra Toplamı	U	p
Kadın	33	70,42	2324	1715,5	0,932
Erkek	105	69,21	7267		

(n: gözlem/kişi sayısı, U: test istatistiği, p: anlamlılık düzeyi)

Çizelge 5.3 incelendiğinde kadın çalışan sıra ortalamasının erkek çalışan sıra ortalamasına göre daha yüksek olduğu görülmekle beraber bu fark istatistiksel olarak anlamlı değildir. Bilgi güvenliği farkındalığında, çalışan bireylerin cinsiyetine göre anlamlı düzeyde farklılaşma olmadığı görülmektedir ($p>0,05$). Bu sonuca göre, “*H3: Erkek çalışanların bilgi güvenliği farkındalığı kadın çalışanlara göre daha yüksektir.*” hipotezi reddedilmiştir.

Bilgi güvenliği farkındalığı çalışmasının, bireylerin yaş grubuna göre Kruskal Wallis H testi sonucu Çizelge 5.4’te görülmektedir.

Çizelge 5.4. Bilgi güvenliği farkındalığının yaş grubuna göre Kruskal Wallis H testi sonucu

Yaş	n	Sıra Ortalaması	sd	χ^2	p
20-29 yaş arası	50	64,01	0,81	1,90	0,592
30-39 yaş arası	60	74,48			
40-49 yaş arası	23	68,98			
50 ve üzeri	5	67,00			

(n: gözlem/kişi sayısı, ss: standart sapma, χ^2 : ki kare değeri/serbestlik derecesi, p: anlamlılık düzeyi)

Çizelge 5.4 incelendiğinde 30-39 yaş arasının sıra ortalama değerlerinin diğer yaş gruplarına ait sıra ortalama değerinden yüksek olduğu görülmekle beraber bu fark istatistiksel olarak anlamlı değildir. Bilgi güvenliği farkındalığında yaş grubuna göre anlamlı düzeyde farklılaşma olmadığı görülmektedir ($p>0,05$). Bu sonuca göre, “*H4: Katılımcıların yaş düzeyi bilgi güvenliği farkındalığı üzerinde etkili değildir.*” hipotezi kabul edilmiştir.

Bilgi güvenliği farkındalığı çalışmasının, öğrenim durumuna göre Kruskal Wallis H testi sonucu Çizelge 5.5’te görülmektedir.

Çizelge 5.5. Bilgi güvenliği farkındalığının öğrenim durumuna göre Kruskal Wallis H testi sonucu

Öğrenim Durumu	n	Sıra Ortalaması	sd	χ^2	p
Lise	1	119,50	0.70	4,21	0,378
Ön Lisans	11	62,68			
Lisans	75	67,10			
Yüksek Lisans	46	71,24			
Doktora	5	94,50			

Çizelge 5.5 incelendiğinde lise mezunu sıra ortalamasının diğer öğrenim durumlarına ait sıra ortalamaya değerlerinden daha yüksek olduğu görülmekle beraber bu fark istatistiksel olarak anlamlı değildir. Bilgi güvenliği farkındalığında, öğrenim durumuna göre anlamlı düzeyde farklılaşma olmadığı görülmektedir ($p>0,05$). Bu sonuca göre, “*H5: Katılımcıların öğrenim durumu bilgi güvenliği farkındalığı üzerinde etkili değildir.*” hipotezi kabul edilmiştir.

Bilgi güvenliği farkındalığının, çalışanların firmadaki pozisyona göre Kruskal Wallis H testi sonucu Çizelge 5.6’da görülmektedir.

Çizelge 5.6. Bilgi güvenliği farkındalığının çalışanların firmadaki pozisyonuna göre Kruskal Wallis H testi sonucu

Pozisyon	n	Sıra Ortalaması	sd	χ^2	p
Yönetici	22	69,32	0,63	1,19	0,551
Teknik personel	81	72,19			
İdari Personel	35	63,39			

Çizelge 5.6 incelendiğinde teknik personel sıra ortalamasının yönetici ve idari personel sıra ortalamasına göre daha yüksek olduğu görülmekle beraber bu fark istatistiksel olarak anlamlı değildir. Bilgi güvenliği farkındalığının, işyerinde çalışılan pozisyona göre anlamlı düzeyde farklılaşma olmadığı görülmektedir ($p>0,05$). Bu sonuca göre, “*H6: Katılımcıların işyerinde çalıştıkları pozisyon bilgi güvenliği farkındalığı üzerinde etkili değildir.*” hipotezi kabul edilmiştir.

Kişilere çalıştıkları firmada bilgi güvenliği hakkında kurs verilme durumuna göre Mann Whitney U testi sonucu Çizelge 5.7’de görülmektedir.

Çizelge 5.7. Bilgi güvenliği farkındalığının firmada konu hakkında eğitim/kurs verilme durumuna göre Mann Whitney U testi sonucu

Grup	n	Sıra Ortalaması	Sıra Toplamı	U	p
Evet	121	73,79	8928	510	0,001
Hayır	17	39,11	663		

Çizelge 5.7 incelendiğinde çalışanlara işyerlerinde bilgi güvenliği farkındalığı hakkında eğitim/kurs verilmesine göre *evet* cevabı verenlerin sıra ortalamasının *hayır* cevabı verenlerin sıra ortalamasına göre çok yüksek olduğu görülmekle beraber bu fark istatistiksel olarak anlamlıdır. Bilgi güvenliği farkındalığında, işyerinde konu hakkında eğitim/kurs verilmesine göre anlamlı düzeyde bir farklılaşma olduğu görülmektedir. ($U = 510$, $p < 0,05$) Çalışmaya katılan kişilerin büyük çoğunluğuna (% 87,7), işyerinde bu konu hakkında eğitim/kurs verilmektedir. Bu sonuca göre, “*H7: Katılımcıların işyerinde aldıkları bilgi güvenliği farkındalık eğitimi/kursu bilgi güvenliği farkındalığı üzerinde etkilidir.*” hipotezi kabul edilmiştir.

Çalışılan işyerinde bilgi güvenliği farkındalığı hakkında kurs verdiğini belirten çalışanların kursu alma sıklığına göre Kruskal Wallis H testi sonucu Çizelge 5.8’de görülmektedir.

Çizelge 5.8. Bilgi güvenliği farkındalığı hakkında eğitim/kurs verilme sıklığına göre Kruskal Wallis H testi sonucu

Sıklık	n	Sıra Ortalaması	sd	χ^2	p
Bir yıldan fazla	15	80,73	0,89	7,10	0,068
Yılda bir	28	51,38			
Altı ayda bir	58	61,72			
Üç ayda bir	20	57,58			

Çizelge 5.8 incelendiğinde Bilgi güvenliği farkındalığı hakkında işyerinde kurs alan çalışanların konu hakkında kurs verilme sıklığındaki gruplar arasındaki sıra ortalama değerlerinin birbirine yakın olduğu görülmektedir. Bilgi güvenliği farkındalığında, işyerinde konu hakkında kurs verilme sıklığına göre anlamlı düzeyde bir farklılaşma olmadığı görülmektedir ($p > 0,05$). Bu sonuca göre, “*H8: Katılımcıların işyerinde aldıkları bilgi güvenliği farkındalık eğitimin/kursun verilmesindeki sıklık derecesi kişilerin bilgi güvenliği farkındalığı üzerinde etkili değildir.*” hipotezi kabul edilmiştir.

Çalışılan işyerinde bilgi güvenliği farkındalığı hakkında eğitim/kurs verildiğini belirten çalışanların aldıkları eğitimin/kursun fayda derecesine göre Kruskal Wallis H testi sonucu Çizelge 5.9’da görülmektedir.

Çizelge 5.9. Bilgi güvenliği farkındalığı hakkında verilen eğitim/kursun fayda derecesine göre Kruskal Wallis H testi sonucu

Fayda Derecesi	n	Sıra Ortalaması	sd	χ^2	p
Faydasız*	5	30,8	0,74	16,96	0,001
Kararsızım*	10	38			
Faydalı*	65	57,06			
Çok Faydalı**	41	76,54			

Çizelge 5.9 incelendiğinde çalışanlara işyerlerinde bilgi güvenliği farkındalığı hakkında verilen eğitim/kursun fayda derecesine göre; çok faydalı cevabını verenlerin sıra ortalamasının faydalı, kararsızım ve faydasız cevaplarını verenlerin sıra ortalamasına göre yüksek olduğu görülmekle beraber bu fark, istatistiksel olarak anlamlıdır. Çok faydalı; faydalı, kararsızım ve faydasıza göre istatistiksel olarak anlamlı farka sahiptir. Bilgi güvenliği farkındalığında, konu hakkında verilen eğitimin/kursun fayda derecesine göre anlamlı düzeyde farklılaşma olduğu görülmektedir. ($p<0,05$). Verilen eğitimin/kursun çalışanlar yarısından fazlası için faydalı bulunmuştur. Bu sonuca göre, “*H9: Katılımcıların işyerinde aldıkları bilgi güvenliği farkındalık eğitiminin/kursunun fayda derecesi kişilerin bilgi güvenliği farkındalığı üzerinde etkilidir.*” hipotezi kabul edilmiştir.

Çalışmada önemli olan sorulardan biri olan işyerinde bilgi güvenliği politikasının var olma durumuna göre Mann Whitney U testi sonucu Çizelge 5.10’da görülmektedir.

Çizelge 5.10. Bilgi güvenliği farkındalığının işyerinde bilgi güvenliği politikasının var olma durumuna göre Mann Whitney U testi sonucu

Grup	n	Sıra Ortalaması	Sıra Toplamı	U	p
Evet	132	72,22	9533,5	36,5	0,000
Hayır	6	9,58	57,5		

Çizelge 5.10 incelendiğinde işyerinde bilgi güvenliği politikasının var olma durumuna göre evet cevabı verenlerin sıra ortalamasının *hayır* cevabı verenlerin sıra ortalamasına göre çok yüksek olduğu görülmekle beraber bu fark istatistiksel olarak anlamlıdır. Bilgi güvenliği farkındalığında, işyerinde bilgi güvenliği politikasının var olma durumuna göre anlamlı düzeyde bir farklılaşma olduğu görülmektedir. ($U= 36,5$, $p<0,05$) Çalışmaya katılan kişilerin büyük çoğunluğunun, işyerinde bilgi güvenliği politikası mevcuttur. Bu sonuca göre, “*H10: İşyerinin bilgi güvenliği politikasına sahip olması kişilerin bilgi güvenliği farkındalığı üzerinde etkilidir.*” hipotezi kabul edilmiştir.

Çalışanların firmalarında bilgi güvenliği politikasının uygulanma derecesi göre Kruskal Wallis H testi sonucu Çizelge 5.11’de görülmektedir.

Çizelge 5.11. Bilgi güvenliği politikasının firmada uygulanma derecesine göre Kruskal Wallis H testi sonucu

Uygulanma Derecesi	n	Sıra Ortalaması	sd	χ^2	p
Hiç uygulanmıyor	1	1	0,81	36,27	0,000
Uygulanmıyor*	4	9,75			
Kararsızım*	12	45,96			
Uygulanıyor*	52	56,84			
Oldukça uygulanıyor**	69	87,59			

Çizelge 5.11 incelendiğinde bilgi güvenliği politikasının uygulanma derecesinde *oldukça uygulanıyor* seçeneğinin sıra ortalamasının; uygulanmıyor, kararsızım ve uygulanıyor seçeneklerinin sıra ortalamasına göre daha yüksek olduğu görülmektedir. Aynı zamanda oldukça uygulanıyor seçeneği sıra ortalamasının hiç uygulanmıyor seçeneğinin sıra ortalamasına göre de oldukça yüksek olduğu görülmektedir. Ancak SPSS veri analiz programı, hiç uygulanmıyor seçeneğini tercih eden kişi katılımındaki düşüklük nedeniyle bu seçeneği ihmal etmiş ve aralarında istatistiksel bir fark çıkartmamıştır. Bilgi güvenliği farkındalığında, bilgi güvenliği politikasının uygulama derecesine göre anlamlı düzeyde farklılaşma olduğu görülmektedir. ($p<0,05$). Bu sonuca göre, “*H11: İşyerinin sahip olduğu bilgi güvenliği politikasının uygulanma derecesi kişilerin bilgi güvenliği farkındalığı üzerinde etkilidir.*” hipotezi kabul edilmiştir.

6. TARTIŞMA VE DEĞERLENDİRME

Çalışma grubunda yer alan kişiler için bilgi güvenliği farkındalık düzeyi kurum türüne göre anlamlı fark oluşturmamaktadır. Bu çalışma için kişilerin kamu kurumu veya özel sektörde çalışmaları bilgi güvenliği farkındalığı üzerinde etkili olan bir etmen değildir. Alanyazında bu durumun incelendiği bir çalışma ile karşılaşılmamıştır. Bu nedenle bu çalışma özgün niteliktedir ve gelecek çalışmalara yeni bir ufuk açacağı düşünülmektedir. Ancak kamu kurumu ve özel sektör çalışanlarının ayrı ayrı bilgi güvenliği farkındalık düzeylerinin ölçüldüğü çalışmalar mevcuttur. Özdemir ve Uluyol'un (2021) çalışmasında, kamu çalışanlarının orta seviye bilgi güvenliği farkındalığına sahip olduğu belirtilmiştir. Taner'in (2019) çalışmasında emniyet çalışanlarının bilgi güvenliği farkındalık düzeyinin düşük olduğu belirtilmiştir. Parsons ve diğerlerinin (2014) çalışmasında, Avustralya'daki kamu kurumu çalışanlarının bilgi güvenliği farkındalığının yeterli seviyede olmadığı ifade edilmiştir. Okul ve diğerlerinin (2018) çalışmasında, konak işletme yöneticilerinin bilgi güvenliği farkındalığının yüksek olduğu belirtilmiştir. Yapılan bu çalışmaların tamamı incelendiğinde; kamu kurumu çalışanlarının bilgi güvenliği farkındalık düzeyi orta ve düşük seviyede çıkarken, özel sektör çalışanlarının yüksek çıktığı gözlemlenmiştir.

Çalışma grubunda yer alan kişilerin bilişim çalışanı olması bilgi güvenliği farkındalık düzeyinde anlamlı fark oluşturmaktadır ve bu çalışmadaki kişilerin bilgi güvenliği farkındalık düzeyi yüksek çıkmıştır. Bu durum; kişilerin sektör farklılığı ayırt etmeksizin bilişim çalışanı olmalarının bilgi güvenliği farkındalık düzeyine olumlu yönde katkı sağladığı gözlemlenmiştir. Alanyazında; Mart'ın (2012), Avcı ve Oruç'un (2020), Teker'in (2019), Yayla'nın (2018), Alemdaroğlu'nun (2020) ve Ceylan'ın (2019) yaptığı çalışmalar ile benzer sonuçlar elde edilmiştir. Bu çalışma, çıkan sonuç itibari ile belirtilen bu çalışmaları desteklemektedir. Ayrıca, bilişim çalışanlarının bilgi güvenliği farkındalık düzeyinin düşük çıktığı bir çalışma ile karşılaşılmamıştır. Yapılan bu çalışmaların tamamı incelendiğinde, bilişim çalışanlarının bilgi güvenliği farkındalık düzeyinin yüksek çıktığı gözlemlenmiştir.

Çalışma grubunda yer alan kişiler için bilgi güvenliği farkındalık düzeyi cinsiyete göre anlamlı fark oluşturmamaktadır. Alanyazında Ceylan'ın (2019), Özdemir ve Uluyol'un (2021), Okul ve diğerlerinin (2018) yaptığı çalışmalar ile benzer sonuçlar elde edilmiştir. Bu çalışma, çıkan sonuç itibari ile belirtilen bu çalışmaları desteklemektedir. Cinsiyet farklılığının bilgi güvenliği farkındalığını etkilediği çalışmalar da mevcuttur. Canoğulları'nın (2021) yaptığı çalışmada, erkek öğretmenlerin bilgi güvenliği farkındalığı

kadın öğretmenlere göre daha yüksektir. Karabatak ve Karabatak'ın (2019) çalışmasında ise erkek okul yöneticilerinin bilgi güvenliği farkındalığı kadın yöneticilere göre daha yüksektir. Dönmez'in (2019), Talan ve Aktürk'ün (2021), Göldağ'ın (2021), Teker'in (2019) çalışmasında, erkek öğrencilerin bilgi güvenliği farkındalığı kız öğrencilere göre daha yüksek çıkmıştır. Çelikçöp ve Yazar'ın (2019), Yılmaz ve diğerlerinin (2016), Solmaz'ın (2020), Keser ve Yayla'nın (2021), Alemdaroğlu'nun (2020), Öztezcan ve Çetinkaya'nın (2017) çalışmasında da erkek katılımcıların bilgi güvenliği farkındalığı kadınlara göre daha yüksek çıkmıştır. Gündüzalp'in (2021) çalışmasında erkeklerin kişisel siber güvenlik farkındalığı kadınlara göre daha yüksek çıkmıştır. Bazı çalışmalarda ise kadın katılımcıların bilgi güvenliği farkındalığı erkek katılımcılara göre daha yüksek çıkmıştır. Çetin'in (2014) çalışmasında, kadınların kişisel verileri yedekleme ve şifreleme, kişisel veri paylaşımı ve risk farkındalığı erkeklere göre daha yüksek çıkmıştır. Mart'ın (2012) çalışmasında, kadın katılımcıların bilgi güvenliği farkındalığı erkeklere göre daha yüksek çıkmıştır. Arıtürk'ün (2015) çalışmasında, kız öğrencilerin bilgi güvenliği farkındalığı erkek öğrencilere göre daha yüksek çıkmıştır. Yapılan tüm bu çalışmalar incelendiğinde, ağırlıklı olarak erkeklerin bilgi güvenliği farkındalığının kadınlardan daha yüksek olduğu gözlemlenmiştir.

Çalışma grubunda yer alan kişiler için bilgi güvenliği farkındalık düzeyi yaşa göre anlamlı fark oluşturmamaktadır. Alanyazında Çelikçöp ve Yazar'ın (2019), Okul ve diğerlerinin (2018), Alemdaroğlu'nun (2020), Teker'in (2019), Öztürk ve Çakır'ın (2022) yaptığı çalışmalar ile benzer sonuçlar elde edilmiştir. Bu çalışma, çıkan sonuç itibari ile belirtilen bu çalışmaları desteklemektedir. Yaş farklılığının bilgi güvenliği farkındalığını etkilediği çalışmalar da mevcuttur. Özdemir ve Uluyol'un (2021), Canoğulları'nın (2021), Bostan ve Akman'ın (2011), Öztezcan ve Çetinkaya'nın (2017) yaptığı çalışmalarda ise bilgi güvenliği farkındalık düzeyi yaşa göre anlamlı fark göstermektedir. Özdemir ve Uluyol'un (2021) çalışmasında 40 yaş altı çalışanların bilgi güvenliği farkındalık düzeyi, 40 yaş üstü katılımcılara göre daha yüksek çıkarken Canoğulları'nın (2021) ile Bostan ve Akman'ın (2011) çalışmalarında yaş ilerledikçe bilgi güvenliği farkındalık seviyesinin düştüğü ifade edilmiştir. Keser ve Yayla'nın (2021), çalışmasında da kişilerin yaşı ilerledikçe bilgi güvenliği farkındalık düzeylerinde düşüş olduğu ifade edilmiştir. Ancak Karadağ ve Abuhanoğlu'nun (2015) çalışmasında, yaşı daha genç katılımcıların bilgi güvenliği farkındalığı yaşı daha ileri katılımcılara göre daha yüksek çıkmıştır. Ceylan'ın (2019) çalışmasında da katılımcıların yaşları ilerledikçe bilgi güvenliği farkındalığının arttığı ifade edilmiştir.

Çalışma grubunda yer alan kişiler için bilgi güvenliği farkındalık düzeyi öğrenim durumuna göre anlamlı fark oluşturmamaktadır. Yılmaz ve diğerlerinin (2015), Ceylan'ın (2019), Okul ve diğerlerinin (2018), Alemdaroğlu (2020), Baran ve Şener'in (2020), Mart'ın (2012) yaptığı çalışmalarda da katılımcıların öğrenim durumu, bilgi güvenliği farkındalık düzeyinde anlamlı bir fark oluşturmamaktadır. Bu araştırma, çıkan sonuç itibari ile bu çalışmaları desteklemektedir. Öğrenim durumu farklılığının bilgi güvenliği farkındalığını etkilediği çalışmalar da mevcuttur. Oktay ve Çakır'ın (2020), Gündüzalp'in (2021) yaptığı çalışmalarda ise bilgi güvenliği farkındalık seviyesinde öğrenim durumuna göre anlamlı fark göstermektedir. Oktay ve Çakır'ın (2020) çalışmasında öğretmenlerin öğrenim düzeyi arttıkça bilgi güvenliği farkındalık seviyelerinin arttığı belirtilmiştir. Gündüzalp'in (2021) çalışmasında, dijital veri güvenliği farkındalığı doktora mezunu çalışanlarda diğer çalışanlara göre daha yüksek iken kişisel siber güvenliği sağlama farkındalığı lisans mezunu çalışanlarda diğer çalışanlara göre daha yüksek olduğu ifade edilmiştir. Öğütçü, Testik ve Chouseinoglou'n (2016) çalışmasında eğitim düzeyi arttıkça bilgi güvenliği farkındalığının arttığı belirtilmiştir. Eğitim düzeyi arttıkça bilgi güvenliği farkındalığının düşüş gösterdiği bir çalışma ile karşılaşılmemiştir. Yapılan tüm bu çalışmalar incelendiğinde, çoğunlukla öğrenim durumunun bilgi güvenliği farkındalığı üzerinde etkili bir etmen olmadığı sonucunun ortaya çıktığı çalışmalar daha fazladır.

Çalışma grubunda yer alan kişiler için bilgi güvenliği farkındalık düzeyi çalıştıkları pozisyona göre anlamlı fark oluşturmamaktadır. Özaslan'ın (2019), Kurt'un (2019), Okul ve diğerlerinin (2018) yaptığı çalışmalarda katılımcıların çalıştıkları pozisyona göre bilgi güvenliği farkındalık düzeyi değişmemiştir. Bu araştırma, çıkan sonuç itibari ile yapılan bu çalışmaları desteklemektedir. Çalışılan pozisyon farklılığının bilgi güvenliği farkındalığını etkilediği çalışmalar da mevcuttur. Eş ve Serdar'ın (2021), Alemdaroğlu'nun (2020) çalışmasında bilgi güvenliği farkındalık seviyesinde iş yerinde çalışılan pozisyon değişkenine göre anlamlı fark göstermektedir. Eş ve Serdar'ın (2021), Alemdaroğlu'nun (2020) çalışmasında; katılımcıların iş yerindeki pozisyonu yükseldikçe bilgi güvenliği farkındalık düzeyinin arttığı ve bu kişilerin sahip olduğu şifreleri daha sık değiştirme tutumlarının olduğu belirtilmiştir. Alanyazında işyerinde çalışılan pozisyonun ilerledikçe kişilerin bilgi güvenliği farkındalığının azaldığına yönelik yapılan bir çalışma ile karşılaşılmemiştir.

Çalışma grubunda yer alan kişiler için bilgi güvenliği farkındalık düzeyi çalıştıkları işyerlerinde eğitim/kurs alınma durumuna göre anlamlı fark oluşturmaktadır. Yayla'nın (2018), Fakeh ve diğerlerinin (2012), Shehri ve Clarke'n (2007), Keser ve Yayla (2021), Akyol ve Uzun'un (2021), Bilen'in (2016), Haeussinger ve Kranz'ın (2013), Hagen ve Albrechtsen'in (2009) yaptığı çalışmalarda katılımcıların bilgi güvenliği farkındalığı hakkında eğitim almaları bilgi güvenliği farkındalık düzeyinde etkili olduğu ifade edilmiştir. Bu araştırma, çıkan sonuç itibari ile yapılan bu çalışmaları desteklemektedir. Yayla'nın (2018) çalışmasında, bilgi güvenliği hakkında eğitim almayan öğretmenlerin bilgi güvenliği farkındalık düzeylerinin daha düşük olduğu belirtilmiştir. Fakeh ve diğerlerinin (2012) çalışmasında çalışanlara yönelik bilgi güvenliği eğitimlerinin bilgi güvenliği farkındalık seviyesini arttırdığı belirtilmiştir. Shehri ve Clarke'n (2007) yaptığı çalışmada güvenlik konusunda eğitim almayan çalışanların bilgi güvenliği farkındalık seviyelerinin eğitim alanlara göre daha düşük olduğu belirtilmiştir. Keser ve Yayla'nın (2021) çalışmasında daha önce bilgi güvenliği farkındalığı eğitimi alan öğretmenlerin farkındalık seviyelerinin eğitim almayanlara göre daha yüksek olduğu belirtilmiştir. Akyol ve Uzun'un (2021) çalışmasında Sağlık Meslek Yüksekokulu öğrencilerinden oluşan çalışma grubunda, bilgi ve iletişim teknolojileri dersi alan öğrencilerle almayanlar arasında bilgi güvenliği farkındalık düzeyi anlamlı fark göstermiştir. Bilen'in (2016) çalışmasında aynı iş yerinde farklı branşlarda çalışan kişiler arasında eğitim alanların almayanlara göre bilgi güvenliği farkındalığının yüksek olduğu belirtilmiştir. Haeussinger ve Kranz'ın (2013) çalışmasında, bilgi güvenliği programlarının özel sektör çalışanlarının bilgi güvenliği farkındalığına ve bilgi güvenliği davranışına katkı sağladığı belirtilmiştir. Hagen ve Albrechtsen'in (2009) çalışmasında, bilgi güvenliği e-öğrenme programlarının, çalışanların bilgi güvenliği farkındalığına olumlu etkide bulunduğu ifade edilmiştir. Bilgi güvenliği farkındalığı için alınan eğitimlerin kişilerin bilgi güvenliği farkındalık düzeyini etkilemediği yönünde çalışmalarda mevcuttur. Karadağ ve Abuhanoğlu'nun (2015) çalışmasında; katılımcıların bilgi güvenliği farkındalık düzeyi, bilgi güvenliği farkındalığı eğitimi alan ve almayan kişiler arasında anlamlı bir fark oluşturmamıştır. Avcı ve Arslan'ın (2019) çalışmasında, alınan hizmet içi bilgi güvenliği farkındalık eğitimlerinin katılımcıların dijital bilgi güvenliği farkındalık seviyesinde anlamlı fark göstermediği belirtilmiştir. Akgün ve Topal'ın (2015) çalışmasında, bilişim güvenliği eğitimi alan öğretmen adayları ile almayanlar arasında bilişim güvenliği farkındalık düzeyi hakkında önemli bir fark gözlenmemiştir. Yapılan bu çalışmaların tamamı incelendiğinde; birçok çalışmada, katılımcıların bilgi güvenliği farkındalığı hakkında aldıkları eğitimin

kişilerin bilgi güvenliği farkındalık düzeyine olumlu katkı sağladığına yönelik sonuçlar ortaya çıkmıştır.

Çalışma grubunda yer alan kişiler için bilgi güvenliği farkındalık düzeyi çalıştıkları işyerlerinde eğitim/kurs verilme sıklık derecesine göre anlamlı fark oluşturmamaktadır. Çalışmadan çıkan bu sonuç Pattinson ve diğerlerinin (2017), Farooq'un (2013), Pattinson ve diğerlerinin (2019) yaptığı çalışmalar ile benzer sonuçlar bulunmuştur. Bu araştırma, çıkan sonuç itibari ile yapılan bu çalışmaları desteklemektedir. Pattinson ve diğerlerinin (2017) yaptığı çalışmada işyerindeki kişilere bilgi güvenliği farkındalığı hakkında eğitim verilme sıklığının farkındalık düzeyine bir etkisi bulunmadığı belirtilmiştir. Farooq'un (2013) çalışmasında; katılımcılara, *bilgi güvenliği farkındalık eğitimi ne sıklıkla almak istediklerinin* sorulduğu soruya verilen cevaplarda ilk sırayı *talep üzerine* seçeneği alırken ikinci sırayı *yılda bir* eğitim alınması gerektiği seçeneği yer almıştır. Ayrıca bu çalışma için katılımcılar arasından bu soruya cevaplayan sadece % 1'i bu eğitimi *sıklıkla* almak istediğini belirtmiştir. Kısaca, kişiler bilgi güvenliği eğitimlerini ihtiyaç duyulduğunda ya da yılda bir almak istemektedir. Pattinson ve diğerlerinin (2019) çalışmasında, bireylerin aldığı bilgi güvenliği eğitiminin bilgi güvenliği farkındalığı üzerine etkisi varken eğitimin alınma sıklığının kişilerin bilgi güvenliği farkındalığı üzerine bir etkisinin bulunmadığı ifade edilmiştir. Bilgi güvenliği farkındalık eğitimi alma sıklığının kişilerin bilgi güvenliği farkındalığına katkı sağladığı bir çalışma ile karşılaşılmamıştır. Yapılan bu çalışmaların incelendiğinde, bilgi güvenliği farkındalığı hakkında verilen eğitimin sıklık derecesinin önemli bir etmen olmadığına yönelik sonuçlar ortaya çıkmıştır.

Çalışma grubunda yer alan kişiler için bilgi güvenliği farkındalık düzeyi çalıştıkları işyerinde verilen bilgi güvenliği farkındalık eğitimi/kursunu faydalı bulunma derecesine göre anlamlı fark oluşturmaktadır. Çalışanlar için verilen bilgi güvenliği farkındalık eğitimi *çok faydalı* bulunmuştur. Stephanou'n (2008), Gökçearslan ve diğerlerinin (2021), Yayla'nın (2018), Tschakert ve Ngamsuriyaroj'ın (2019), Bauer ve diğerlerinin (2017) yaptığı çalışmalar ile benzer sonuçlar elde edilmiştir. Bu araştırma, çıkan sonuç itibari ile yapılan bu çalışmaları desteklemektedir. Stephanou'n (2008) çalışmasında, bilgi güvenliği farkındalık eğitiminin kişinin doğru bilgi güvenliği davranışı sergilemesine olumlu katkı sağladığı belirtilmiştir. Gökçearslan ve diğerlerinin (2021), Yayla'nın (2018) yaptığı çalışmalarda; katılımcılar bilgi güvenliği farkındalığı hakkında alınan ders ve eğitimleri faydalı bulmuşlardır. Gökçearslan ve diğerlerinin (2021) çalışmasında ortaokul öğrencileri için bilişim teknolojileri dersinden alınan faydanın bilgi güvenliği farkındalık düzeyini

etkilediği belirtilmiştir. Yayla'nın (2018) çalışmasında, öğretmenler aldıkları bilgi güvenliği farkındalığı eğitimlerinin kendilerinin bilgi güvenliği farkındalık düzeyleri için yeterli olduğunu ifade ederek bu durum anlamlı bir fark oluşturmuştur. Tschakert ve Ngamsuriyaroj'ın (2019) çalışmasında, *kimlik avı* konulu eğitimin, eğitimi alan kişilerce faydalı bulunduğu belirtilmiştir. Bauer ve diğerlerinin (2017) çalışmasında, bilgi güvenliği yöneticilerinin bilgi güvenliği farkındalık programlarını yararlı buldukları belirtilmiştir. Alanyazında, alınan bilgi güvenliği farkındalığı eğitimlerinin yetersiz görüldüğü ve kişilerin bilgi güvenliği farkındalığına katkı sağlamadığına yönelik yapılan çalışmalarla karşılaşılmamıştır. Yapılan bu çalışmaların tamamı incelendiğinde, bilgi güvenliği farkındalığı eğitimlerinin kişilerin bilgi güvenliği farkındalığına olumlu katkı sağladığına yönelik sonuçlar ortaya çıkmıştır.

Çalışma grubunda yer alan kişiler için bilgi güvenliği farkındalık düzeyi çalıştıkları işyerinde bilgi güvenliği politikasının olma durumuna göre anlamlı fark oluşturmaktadır. Katılımcıların büyük çoğunluğunun (% 95,69) işyerinde bilgi güvenliği politikası vardır. Araştırmadan çıkan bu sonuç; Yıldırım'ın (2006), Meral ve Bülbül'ün (2021), Bulgurcu ve diğerlerinin (2009), Haeussinger ve Kranz'in (2013), Chan ve Mubarek'in (2012) yaptığı çalışmaları desteklemektedir. Yıldırım'ın (2006) çalışmasında bankaların yarısından fazlasının (3/2) bilgi güvenliği politikasına sahip olduğunu ve bu politikanın banka için iç denetim ile risk yönetimine katkıda bulunduğu ifade edilmiştir. Meral ve Bülbül'ün (2021) çalışmasında, bilgi güvenliği politikasının işyerlerinde kurumsal bilgi güvenliğinin sağlanmasına yardımcı olduğu belirtilmiştir. Bulgurcu, Çavuşoğlu ve Benbasat'ın (2009) çalışmasında, bilgi güvenliği farkındalığının bilgi güvenliği politikası üzerindeki olumlu etkileri ifade edilmiştir. Haeussinger ve Kranz'in (2013) çalışmasında, bilgi güvenliği farkındalığı ile bilgi güvenliği politikası arasındaki uyum etkisi incelenmiş ve bu iki unsurun birbirlerini geliştirdiği vurgulanmıştır. Chan ve Mubarek'in (2012) çalışmasında, yönetsel olarak bilgi güvenliği farkındalığı eksikliğinin, bilgi güvenliği politikasını olumsuz etkilediği belirtilmiştir. İşyerinin bilgi güvenliği politikasına sahip olmasının çalışanların bilgi güvenliği farkındalık düzeyinde anlamlı bir farka neden olmayan çalışmalarda mevcuttur. Örneğin, Gebru'nun (2020) çalışmasında; Etiyopya'daki özel banka çalışanların işyerinde % 98 oranında bilgi güvenliği politikası bulunmasına rağmen çalışanların bilgi güvenliği farkındalığı düşük çıkmıştır. Yapılan bu çalışmaların tamamı incelendiğinde; çoğu çalışmada, işyerinin bilgi güvenliği politikasına sahip olması çalışanların bilgi güvenliği farkındalığına olumlu katkı sağladığına yönelik durumlar gözlemlenmiştir.

Çalışma grubunda yer alan kişiler için bilgi güvenliği farkındalık düzeyi çalıştıkları işyerinde bilgi güvenliği politikasının uygulanma derecesine göre anlamlı fark oluşturmaktadır. Katılımcılar işyerinde var olan bilgi güvenliği politikasının işyerlerinde *oldukça uygulandığını* ifade etmişlerdir. Araştırmadan çıkan bu sonuç; Gebru (2020), Bulgurcu ve diğerlerinin (2010) yaptığı çalışmaları desteklemektedir. Gebru (2020), Etiyopya'daki özel banka çalışanlarının bilgi güvenliği farkındalığını etkileyen etmenler üzerine bir çalışma yürütmüştür. Çıkan sonuçta, banka çalışanlarının bilgi güvenliği farkındalık düzeyleri düşük çıkmıştır. Bunun nedeni, kişilerin işyerlerindeki bilgi güvenliği politikasının yeterince uygulanmamasıdır. Gebru (2020) çalışmasında, kişilerin bilgi güvenliği farkındalığının artırılması için kurumsal bilgi güvenliği politikasının yönetsel olarak uygulanması ve çalışanlara uygulanması gerektiği hakkında öneride bulunulmuştur. Bulgurcu ve diğerlerinin (2010) çalışmasında, çalışanların bilgi güvenliği farkındalığının işyerindeki bilgi güvenliği politikasına uyum gösterme konusunda etkili olduğu ifade edilmiştir. Yapılan bu çalışmaların tamamı incelendiğinde; tümünün işyerinde sahip olunan bilgi güvenliği politikasının uygulanma durumunun, çalışanların bilgi güvenliği farkındalığını etkilediğine yönelik durumlar gözlemlenmiştir.

Kurulan hipotezlerin alanyazın çalışmaları ve yapılan bu çalışma için kabul edilme ve reddedilme durumu Çizelge 6.1'de görülmektedir.

Çizelge 6.1. Kurulan hipotezlerin çalışmalarda kabul edilme/reddedilme durumu

Yapılan Alanyazın Çalışmaları	H1	H2	H3	H4	H5	H6	H7	H8	H9	H10	H11
Yıldırım (2006)										✓	
Shehri ve Clarke (2007)							✓				
Stephanou (2008)									✓		
Bulgurcu ve diğerleri (2009)										✓	
Hagen ve Albrechtsen (2009)							✓				
Bulgurcu ve diğerleri (2010)											✓
Bostan ve Akman (2011)				x							
Chan ve Mubarek (2012)										✓	
Fakeh ve diğerleri (2012)							✓				
Mart (2012)		✓	x		✓						
Farooq (2013)								✓			

Çizelge 6.1. (devamı) Kurulan hipotezlerin çalışmalarda kabul edilme/reddedilme durumu

Haeussinger ve Kranz (2013)							✓			✓	
Çetin (2014)			x								
Aritürk (2015)			x								
Akgün ve Topal (2015)							x				
Karadağ ve Abuhanoğlu (2015)				x			x				
Bilen (2016)							✓				
Öğütçü, Testik ve Chouseinoglou (2016)					x						
Yılmaz ve diğerleri (2016)			✓		✓						
Bauer ve diğerleri (2017)									✓		
Pattinson ve diğerleri (2017)								✓			
Öztezcan ve Çetinkaya (2017)				x							
Yayla (2018)		✓					✓		✓		
Okul ve diğerleri (2018)			x	✓	✓	✓					
Avcı ve Arslan (2019)							x				
Çelikçöp ve Yazar (2019)			x	✓							
Dönmez (2019)			✓								
Ceylan (2019)		✓	x	x	✓						
Karabatak ve Karabatak (2019)			✓								
Pattinson ve diğerleri (2019)								✓			
Tschakert ve Ngamsuriyaroj (2019)									✓		
Özaslan (2019)						✓					
Kurt (2019)						✓					
Teker (2019)		✓	✓	✓							
Avcı ve Oruç (2020)		✓									
Alemdaroğlu (2020)		✓	✓	✓							
Gebbru (2020)										x	✓
Oktay ve Çakır (2020)					x	x					
Baran ve Şener (2020)					✓						
Solmaz (2020)			✓								
Meral ve Bülbül (2021)										✓	
Eş ve Serdar (2021)						x					
Gökçearslan ve diğerleri (2021)									✓		
Özdemir ve Uluyol (2021)			x	x							
Talan ve Aktürk (2021)			✓								
Canoğulları (2021)			✓	x							

Çizelge 6.1. (devamı) Kurulan hipotezlerin çalışmalarda kabul edilme/reddedilme durumu

Göldağ (2021)			✓								
Keser ve Yayla (2021)			✓				✓				
Gündüzalp' (2021)			✓		x						
Akyol ve Uzun (2021)							✓				
Öztürk ve Çakır (2022)				✓							
Nezgitli (2022)	x	✓	x	✓	✓	✓	✓	✓	✓	✓	✓

Alanyazında kişilerin bilgi güvenliği farkındalığına etkileyen etmenler incelenirken demografik özelliklerden; cinsiyet ve yaş değişkeni çalışmaların çoğunlukta yer almaktadır. Ancak cinsiyet veya yaş farklılığının, kişilerin bilgi güvenliği farkındalığı üzerinde etkili olduğu çalışmalarda bu durumun sonucunun neden böyle çıktığına dair kapsamlı bir ölçme yapılmamıştır. Alanyazında; öğrenim durumu, işyerinde çalışılan pozisyon farklılığı gibi demografik özelliklerin kişilerin bilgi güvenliği farkındalığı üzerine olan etkisinin ölçüldüğü çalışma sayısı cinsiyet ve yaş değişkenine göre daha azdır. Öğrenim durumu ve pozisyon farklılığının kişilerin bilgi güvenliği farkındalığına olan ilişkisinin incelendiği çalışmalarda detaylı bir ölçüm yapılmamıştır. Kısacası; alanyazında kişilerin bilgi güvenliği farkındalığı ve demografik özellikleri arasındaki ilişki incelenirken neden sonuç ilişkilerinde eksiklikler mevcuttur. Ayrıca bilgi güvenliği farkındalığı için belli demografik sorular belirlenmiş ve bunların kapsamı genişletilmemiştir. Alanyazında mevcut olan diğer bir sorun ise kişilerin bilgi güvenliği farkındalığı ile işyerindeki bilgi güvenliği politikası ve bu politikanın uygulanması arasındaki ilişkinin ele alındığı çalışmaların sayısındaki azlıktır. Çalışmalar ya demografik özelliklere ya da bilgi güvenliği politikasına odaklanarak kişilerin bilgi güvenliği farkındalığını ölçmek istemiştir. Demografik özellikler, bilgi güvenliği politikasının varlığı ve bilgi güvenliği politikasının uygulanması ile kişilerin bilgi güvenliği farkındalığı hakkında ilişkinin kurulduğu bir çalışma mevcut değildir. Bu nedenle; yapılan çalışmalar; belirli başlı etmenlerin bilgi güvenliği farkındalığı üzerine olan etkilerini ölçen ancak kapsamlı olmayan kendini tekrar eden çalışmalar olarak yer almaktadır. Bu çalışma hem demografik özellikler hem de bilgi güvenliği politikası ve ayrıca kurum türü gibi farklı bir etmenin bilgi güvenliği farkındalığı üzerine etkisini araştıran kapsamlı ve özgün bir çalışmadır.



7. SONUÇ VE ÖNERİLER

Bu bölümde, araştırmanın sonuç ve önerilere yer verilmiştir. Araştırmadan çıkan sonuçlara bakıldığında; kamu kurumu ve özel sektör çalışanlarına yönelik bilgi güvenliği farkındalığı üzerine etkili olan ve olmayan etmenler mevcuttur. Katılımcıların bilgi güvenliği farkındalığı üzerinde etkili olmayan etmenler; kurum türü, cinsiyet, yaş, öğrenim durumu, işyerinde çalışılan pozisyon, bilgi güvenliği farkındalığı hakkında verilen eğitimin/kursun sıklık derecesi olmuştur. Çalışmanın temel amacını oluşturan kurum türünün katılımcılar için bilgi güvenliği farkındalığı üzerinde anlamlı bir etkisinin olmamasının nedeni; kişilerin bilişim çalışanı olmasıdır. Ayrıca katılımcıların bilişim çalışanı olduğu için bilgi güvenliği farkındalık düzeyleri yüksektir. Çalışma kapsamında katılımcıların bilgi güvenliği farkındalığı üzerinde etkili olan dört etmen dikkat çekmektedir. Bunlar;

- İşyerinde alınan bilgi güvenliği farkındalık eğitimi,
- Alınan bu eğitimin fayda derecesi,
- İşyerinin bilgi güvenliği politikasına sahip olması
- Bu politikanın uygulanma derecesidir.

Kamu kurumu ve özel sektör çalışanlarına yönelik bilgi güvenliği farkındalığı üzerine alınan eğitim/kurs gibi faaliyetlerin önemli ve yararlı olduğu katılımcılar tarafından belirtilmiştir. Bu eğitim/kurslar bilgi güvenliği farkındalığının oluşması ve ona ait kavramların algılanması için önemli bir araç olmaktadır. Çalışanlar için alınan eğitimlerin/kursların hangi sıklıkla alındığı değil bu faaliyetlerin niteliği ön plana çıkmaktadır. Bilinçlendirme faaliyetlerinin yanı sıra çalıştıkları işyerlerinde kurumsal bilgi güvenliği politikasının olması da çalışanlar için farkındalık düzeyini belirleyen başka bir etmendir. Sadece kurumsal bilgi güvenliği politikasının var olması yeterli görülmemekle beraber bu politikanın etkin şekilde uygulanması da çalışanların bilgi güvenliği farkındalığında önemlidir. Kısaca, çalışanların bilgi güvenliği farkındalığının belirleyen bu dört etmenin etkin bir şekilde uygulanması, işyeri çalışanları için bilgi güvenliği farkındalık düzeyine olumlu yönde katkıda bulunmuştur. Bu sonuçlar doğrultusunda şu önerilerde bulunulmuştur:

- Cinsiyet, yaş, öğrenim durumu, işyerindeki pozisyon farklılığı, çalışanlar arasında kurumsal bilgi güvenliği farkındalık düzeyinin belirlenmesinde etkili olmamıştır. Bu

nedenle; ileride yapılacak çalışmalar, çalışanların demografik özelliklerine ek olarak bireysel özelliklerine, kurum kültürüne ve ülke politikasına yönelik yürütülebilir.

- İleride yapılacak çalışmalar için bilgi güvenliği farkındalığı eğitimlerinde, farklı öğretim yöntemleri (uzaktan eğitim, mobil veya karma öğrenme yaklaşımları gibi) üzerine araştırmalar yürütülebilir.
- Kurum türündeki farklılık, çalışanlar arasında kurumsal bilgi güvenliği farkındalık düzeyinin belirlenmesinde etkili olmamıştır. Bu nedenle, ileride yürütülecek çalışmalar, kurum türü farklılığına ek olarak kurumsal yapılanma farklılığı konusuna odaklanarak yürütülebilir.
- Çalışanlar için kurumsal bilgi güvenliği farkındalık düzeyinin belirlenmesi için kişilerin bu konu hakkındaki durumları çeşitli yöntemlerle (anket, ölçek vb.) ölçümlenebilir. Bu durum, çalışanların bilgi güvenliği farkındalığı potansiyellerinin belirlenmesi için önem arz edebilir ve bu ölçümleme faaliyetlerinin işyerleri için yapılması önerilmektedir.
- İşyerinde alınan bilgi güvenliği farkındalık eğitim/kurs faaliyetleri çalışanlar arasında kurumsal bilgi güvenliği farkındalık düzeyinin belirlenmesinde etkili olmuştur. Bu nedenle, işyeri çalışanlarına yönelik bilgi güvenliği farkındalığı eğitimlerine önem vererek başta yapacakları ölçümleme çalışmaları ile çalışanların ihtiyaçları doğrultusunda bu eğitimleri planlanmaları önerilmektedir.
- Alınan eğitim/kurs faaliyetlerinin fayda derecesi çalışanlar arasında kurumsal bilgi güvenliği farkındalık düzeyinin belirlenmesinde etkili olurken alınan eğitim/kurs faaliyetlerinin sıklık derecesi etkili olmamıştır. Bu nedenle; işyerleri, çalışanlarına bilgi güvenliği farkındalığı konusunda eğitim/kurs verirken bu faaliyetlerin hangi sıklıkla verildiğine odaklanmak yerine bu faaliyetlerin kişiler için fayda sağlamasına odaklanmalıdır. Bu hususta, verilen eğitim/kurs faaliyetlerinin faydalı olup olmadığının belirlenmesi için hem eğitimi veren eğitmenden hem de katılımcılardan geri bildirim alınması ileride planlanan bilgi güvenliği farkındalığı çalışmalarına yeni bir yol haritası çizmeye yardımcı olacağından işyerinin bu hususları dikkate alması önerilmektedir.
- Çalışanların işyeri tarafından düzenlenen bilgi güvenliği farkındalığı eğitim/kurs faaliyetlerine katılmaları ve faaliyet sonunda görüşlerini şeffaf biçimde belirterek düzenlenecek yeni faaliyetlere katkı sağlamaları önerilmektedir.

- İşyerleri için kurumsal bilgi güvenliği farkındalığı kapsamında yürütülen faaliyetler sadece eğitim/kurs faaliyetleri ile sınırlandırılmayabilir. Bu faaliyet alanlarının kapsamı, işyeri çalışanlarının ihtiyaçları doğrultusunda; çeşitli programlar, etkinlikler (seminer, toplantı, çalıştay vb.), farklı bölüm çalışanları arasında oluşturulacak grup çalışmaları ile desteklenebilir.
- İşyeri; çalışanlarının cinsiyet, yaş, öğrenim durumu, çalıştıkları pozisyon farklılığına bakmadan düzenlenen bilgi güvenliği farkındalık faaliyetine kişileri dâhil etmesi önerilmektedir.
- İşyerinin çalışanları için bilgi güvenliği farkındalığı üzerine eğitim/kurs faaliyetleri yürütmesi faydalıdır ancak tek başına yeterli değildir. Bu faaliyetlerin yol haritasının belirleneceği kurumun sahip olması gereken bazı planlamalara ihtiyaç duyulmaktadır. Bu nedenle, işyerinin kurumsal bilgi güvenliği politikasına sahip olması çalışanlar arasında kurumsal bilgi güvenliği farkındalık düzeyinin belirlenmesinde etkili olmuştur. Kurumsal bilgi güvenliği politikası, kurumsal bilgi güvenliği farkındalık faaliyetlerini içine alarak planlanan etkinlikleri içermektedir. Bu hususta, işyerlerinin bilgi güvenliği politikasına sahip olması önerilmektedir.
- Kurumsal bilgi güvenliği politikasının uygulanma derecesi çalışanlar arasında kurumsal bilgi güvenliği farkındalık düzeyinin belirlenmesinde etkili olmuştur. Bu nedenle; işyerinin kurumsal bilgi güvenliği politikasına sahip olması çalışanların bilgi güvenliği farkındalık düzeyini arttırmak için tek başına yeterli olmamakla birlikte bu politikanın etkin kullanılması ve tüm çalışanların ihtiyaçlarını karşılayacak şekilde olması önerilmektedir. Çalışanların bilgi güvenliği farkındalık düzeyinin artırılması için kurum yönetici/yöneticilerinin bilgi güvenliği politikasını uygulanması ve bu politikanın çalışanlar tarafından uygulanma durumunu takip etmesi önerilmektedir.



KAYNAKLAR

- Acar, H. (2019). *Rehberlik ve araştırma merkezinde çalışan öğretmenlerin genel özyeterlilik algıları ve iş doyumunu düzeylerinin incelenmesi*. Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.
- Acılar, A. (2009). İşletmelerde bilgi güvenliği ve örgüt kültürü. *Organizasyon ve Yönetim Bilimleri Dergisi*, 1(1), 34-46.
- Açıkgöz, E. İ. (2020). *Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu (TCK m. 244/4)*. (Birinci Baskı). Türkiye: Adalet Basım Yayım Dağıtım.
- Ada, M. (2018). *NATO üyesi ülkelerin siber güvenlik stratejileri açısından incelenmesi*. Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara.
- Akbal, E. ve Doğan, Ş., Tuncer, T. ve Atalay, N. S. (2019). Adli bilişim alanında ağ analizi. *Bitlis Eren Üniversitesi Fen Bilimleri Dergisi*, 8(2), 582-594.
- Akbal, E. ve Güneş, F. (2016). Adli bilişim mühendisliği eğitiminin kurumlar açısından önemi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 4(2), 395-402.
- Akcan, G. E. (2019). *Özel sağlık sigorta şirketleri çalışanlarının elektronik sağlık kayıtlarının gizliliği ve güvenliği hakkında görüşlerinin değerlendirilmesi*. Doktora Tezi, Marmara Üniversitesi Sağlık Bilimleri Enstitüsü, İstanbul.
- Aktan, E. ve Aydın, B. (2016). Cameron-Freeman örgüt kültürü türleri ekseninde örgüt kültürü ve bilgi güvenliği algısı ilişkisi: Devlet üniversitelerinde bir uygulama. *İşletme Araştırmaları Dergisi*, 8(4), 324-344.
- Akyol, E. ve Uzun, Y. (2021) Bilgi ve iletişim teknolojisi dersi alan yüksekokul öğrencilerinin bilişim güvenliği farkındalığı: Ufuk Üniversitesi Sağlık Hizmetleri Meslek Yüksekokulu örneği. *Ufuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 10(19), 69-83.
- Aladağ, C. E., Kurtarangel, E. ve Bahtiyar, Ş. (2014). Medikal bilgi sistemlerinde güvenlik, mahremiyet ve kimlik doğrulama. *Akademik Bilişim*, 273-277.
- Alagöz, A. ve Allahverdi, M. (2011). Kurumsal bilgi güvenliği ve muhasebe bilgi sistemi. *Muhasebe ve Vergi Uygulamaları Dergisi (MUVU)/Journal of Accounting and Taxation Studies (JATS)*, 4(3), 47-64.
- Alemdaroğlu, A. (2020). *Çalışanların bilgi güvenliği farkındalığına ilişkin algıları: bankacılık sektöründe bir araştırma*. Yüksek Lisans Tezi, İstinye Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Al-Awadi, M. ve Renaud, K. (2007). Success factors in information security implementation in organizations. *In IADIS International Conference e-Society*, 169-176.
- AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in human behavior*, 49, 567-575.

- Alkan, M., Atalay, A.H., Canbek, G. ve Bilirgen, C. (2012). Türkiye ulusal siber güvenlik stratejisi önerisi. Proje: ulusal/uluslararası siber güvenlik. *Bilgi Güvenliği Derneği*. 1-34.
- AlMindeel, R., ve Martins, J. T. (2020). Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. *Information Technology ve People*, 34(2), 770-788.
- Alotaibi, M., Furnell, S., and Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 352-358
- Al-Rashdi, Z. A. A. (2018). *Information security accountability in the cloud computing context*. Doktora Tezi, RMIT Üniversitesi, Avustralya.
- Al-Sanabani, H. (2016). *Eklentiler kullanarak veri kaybını engelleme*. Yüksek Lisans Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya.
- Altın, N. ve Görgün, A. (2014). Akıllı şebekelerde siber güvenlik uygulamaları. *Gazi Üniversitesi Fen Bilimleri Enstitüsü*, 1-38.
- Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice* (İkinci Baskı). United Kingdom: Syngress.
- Arda, E. (2020). *Siber uzay ortamında saldırı tehditlerinin farkındalığı, tespiti ve önlenmesi üzerine bir gerçek zaman sistem önerisi*. Yüksek Lisans Tezi, Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
- Arıtürk, M. (2015). Bilgi farkındalığı ve bilgi güvenliğinin karşılaştırılması. *XVII. Akademik Bilişim Konferansı*, Eskişehir.
- Arslan, M. E. (2016). Siber güvenlik ve siber saldırı türleri. *Academia*, 1-10.
- Aslan, S. (2019). *Bilişim teknolojileri alanındaki meslek lisesi öğrencilerinin siber güvenliğe yönelik bilgi düzeylerinin belirlenmesi*. Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi, Eğitim Bilimleri Enstitüsü, Konya.
- Avcı, Ü. ve Arslan, E. (2019). Dijital veri güvenliği farkındalığı ve bilgi okuryazarlığı ile alınan hizmet içi eğitimin etkisi. *Ankara University Journal of Faculty of Educational Sciences (JFES)*, 52(3), 891-914.
- Avcı, Ü. ve Oruç, O. (2020) Üniversite öğrencilerinin kişisel siber güvenlik davranışları ve bilgi güvenliği farkındalıklarının incelenmesi. *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, 21(1), 284-303.
- Ballı, F. E. ve Önder, E. (2019) Çeşitli değişkenler açısından öğretmenlerin örgütsel yaratıcılık algılarının incelenmesi. *14. Uluslararası Eğitim Yönetimi Kongresi Tam Metin Bildiri Kitabı*, 518-522.

- Baran, S. ve Şener, E. (2020). Örgütlerde bilgi güvenliğini etkileyen bir unsur: Örgütsel bilgi paylaşımı. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (41), 410-427.
- Bartos, C. A. (2016). Cyber weapons are not created equal. *In US Naval Institute Proceedings*, 142(6), 30-33.
- Bauer, S., Bernroider, E. W., ve Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *computers ve security*, 68, 145-159.
- Başlar, Y. (2019). Adli bilişim sürecinde karşılaşılan sorunlar ve çözüm önerileri. *TBB Dergisi*.
- Baykara, M., Daş, R. ve Gürkan, T. (2016). Web sunucu erişim kütüklerinden web ataklarının tespitine yönelik web tabanlı log analiz platformu. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 28(2), 291-302.
- 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)*, 231-239.
- Bayraktar, R. (2020). İyileştirme kuramı bağlamında geleneksel TV'den IPTV'ye dönüşen izleyici tercihleri: Literatür üzerine teorik bir inceleme. *Atatürk İletişim Dergisi*, (19), 79-93.
- Bıçakcı, S. (2012). Yeni savaş ve siber güvenlik arasında NATO'nun yeniden doğuşu. *Uluslararası İlişkiler Dergisi*, 9(34), 205-226.
- Bıçakcı, S. (2014). NATO'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. *Uluslararası İlişkiler Dergisi*, 10(40), 100-130.
- Bilen, A. (2016). *Bir kurumun bilgi güvenliği farkındalığının incelenmesi*. Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ.
- Bingöl, U. (2010). *ISO 27001 Bilgi Güvenliği Yönetim Sistemi Otomasyonu*. Yüksek Lisans Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya.
- Blakley, B., McDermott, E., and Geer, D. (2001). Information security is information risk management. *In Proceedings of the 2001 workshop on New security paradigms*, 97-104.
- Bland, J. M. ve Altman, D. G. (1997). Statistics notes: Cronbach's alpha. *Bmj*, 314(7080), 570-572.
- Bostan, A. ve Akman, İ. (2011). Kullanıcı açısından bir durum tespiti. *IV. Ağ ve Bilgi Güvenliği Sempozyumu Bildiriler Kitabı*, 51-55.
- Brenner, S. W. (2004). Toward a criminal law for cyberspace: distributed security. *BUJ Sci. and Tech. L.*, 10, 1.

- Bulgurcu, B., Çavusoglu, H., ve Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. *AMCIS 2009 Proceedings*, 419.
- Bulgurcu, B., Çavusoglu, H., ve Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.
- Büyüköztürk, Ş. (2002). *Sosyal bilimler için veri analizi el kitabı*. (Genişletilmiş Ondokuzuncu Baskı) Türkiye: Pegem Akademi.
- Büyüköztürk, Ş. (2010) *Sosyal bilimler için veri analizi el kitabı*. (Onbirinci Baskı) Türkiye: Pegem A Yayıncılık.
- Can, Ö. ve Akbaş, M. (2014). Kurumsal ağ ve sistem güvenliği politikalarının önemi ve bir durum çalışması. *TÜBAV Bilim Dergisi*, 7(2), 16-31.
- Canbek, G. ve Sağiroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9(3), 165-174.
- Canbek, G., Sağiroğlu, Ş. ve Baykal, N. (2013), Bilgisayar ağlarından yazılıma: Bütüncül siber güvenlik yaklaşımı, *1 st International Symposium on Digital Forensics and Security (ISDFS'13)*, 126-130.
- Canoğulları, E. (2021). Öğretmenlerin bilgi güvenliği konusundaki farkındalıklarının incelenmesi. *Kalem Eğitim ve İnsan Bilimleri Dergisi*, 11(2), 651-679.
- Cervantes, G. V. and Fenz, S. (2014). How to assess confidentiality requirements of corporate assets? *In IFIP International Information Security Conference*, 428, 234-241.
- Ceylan, H. 2019. *Türkiye’de bilgi güvenliği algısının istatistiksel analizi*. Yüksek Lisans Tezi, İstanbul Üniversitesi Cerrahpaşa Adli Tıp ve Adli Bilimler Enstitüsü, İstanbul.
- Chan, H. ve Mubarak, S. (2012). Significance of information security awareness in the higher education sector. *International Journal of Computer Applications*, 60(10).
- Chang, S. E. ve Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial management ve data systems*.1-34.
- Charney, S. ve Alexander, K. (1996). Computer crime. *Emory LJ*, 45, 931.
- Cherdantseva, Y. ve Hilton, J. (2013). A reference model of information assurance and security. *In 2013 International Conference on Availability, Reliability and Security*, 546-555.
- Cisco (2020), *Cisco Annual Internet Report (2018-2023)*.
- Connolly, Y., Lang, L. Gathegi, M. J. ve Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study.

Information ve Computer Security, 25(2), 118-136.

- Çağlayan, U. (2003). Bilgi güvenliği: Dünyadaki eğilimler. *Ulaknet Sistem Yönetimi Konferansı*. Ankara.
- Çakır, H. ve Tuygun, M. (2019). ISO27001 bilgi güvenliği yönetim sistemi standardının kamu kurumlarına uygulanabilirliğinin araştırılması: Ankara ili örneği. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 3(2), 59-78.
- Çakır, S. ve Kesler, M. (2012). Bilgisayar güvenliğini tehdit eden virüsler ve antivirüs yazılımları. *XIV. Akademik Bilişim Konferansı Bildirileri*, 551, 558.
- Çalık, D. ve Çınar, Ö. P. (2009). Geçmişten günümüze bilgi yaklaşımları bilgi toplumu ve internet. *XIV. Türkiye'de İnternet Konferansı Bildirileri*, 77-88.
- Çalışkan, M. (2014). *Sanallaştırma teknolojilerinin saldırı tespit ve önleme sistemlerinin performansı üzerine etkisi*. Yüksek Lisans Tezi, Hava Harp Okulu Havacılık ve Uzay Teknolojileri Enstitüsü, İstanbul.
- Çalışkan, S. (2014). Pozitif örgütsel davranış değişkenleri ile yeni araştırma modelleri geliştirme arayışları: Pozitif örgütsel davranış değişkenlerinin işe adanmışlık, tükenmişlik ve sinizm üzerine etkileri ve bu etkileşimde örgütsel adalet algısının aracılık rolü üzerine bir araştırma. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 16(3), 363-382.
- Çam, H., Aslay, F. ve Özen, Ü. (2019). Yükseköğretim kurumlarında bilgi güvenliği farkındalık düzeylerinin ölçülmesi. *Yönetim Bilişim Sistemleri Dergisi*, 5(2), 1-11.
- Çatuk, C. (2018). *Siber riskler karşısında KOBİ'lerin bilgi güvenliği farkındalıklarını ölçen bir ölçek geliştirme: Gaziantep örnekleme*. Doktora Tezi, Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü, Gaziantep.
- Çelikçöp, Ç. ve Yazar, Y. (2019). Kalite yönetim direktörlerinin bilgi güvenliği farkındalığı: İstanbul ili örneği. *Sağlıkta Performans ve Kalite Dergisi*, 17(2), 29-48.
- Çetin, H. (2014). Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi. *Akdeniz İİBF Dergisi*, 14(29), 86-105.
- Çetinkaya, L., Güldüren, C., ve Keser, H. (2017). Öğretmenler için bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *Milli Eğitim Dergisi*, 46(216), 33-52.
- Çetinkaya, M. (2008). Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin uygulanması. *Akademik Bilişim*, 511-516.
- Çotuksöken, B. (2018). *Antropontoloji ya da insan varlık bilgisi*. Türkiye: Notos Kitap Yayınevi, İstanbul.
- Demir, B. (2005). Muhasebe bilgi sistemlerinde bilgi güvenliği. *Muhasebe ve Finansman Dergisi*, (26), 147-156.
- Demirel, M., Işık, U., Demirel, D. H., Üstün, Ü. D. ve Gümüşgöl, O. (2016). Gelecek zaman

- algısı: Beden eğitimi ve spor yüksekokulu öğrencilerine yönelik bir çalışma. *İstanbul Üniversitesi Spor Bilimleri Dergisi*, 6(1), 10-20.
- Demirtaş, H. (2013). *Bilgi güvenliği Yönetiminin gerekleri ve başarı dayanakları: bir uygulama örneği*. Yüksek Lisans Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya.
- Denerel, C. (2016). Güvende olmak için uyumlu ol. *CyberMag Dergisi*, 6.
- Dhillon, G. (1999) Managing and controlling computer misuse. *Information Management ve Computer Security*, 7(4), 171-175.
- Dijle, H. ve Doğan, N. (2011). Türkiye’de bilişim suçlarına eğitilmiş insanların bakışı. *Bilişim Teknolojileri Dergisi*, 4(2), 43-53.
- Diler, R. (2014). Mahremiyet eğitimi ve önemi. *Gaziosmanpaşa Üniversitesi İlahiyat Fakültesi Dergisi*. 2(1), 69-98.
- Dlamini, M. T., Eloff, J. H. ve Eloff, M. M. (2009). Information security: The moving target. *Computers ve security*, 28(3-4), 189-198.
- Doğantimur, F. (2009). *ISO 27001 standardı çerçevesinde kurumsal bilgi güvenliği*. Mesleki Yeterlilik Tezi, TC Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Ankara.
- Dönmez, G. (2019). *Lise öğrencilerinin bilgi güvenliği farkındalığı ile dijital okuryazarlığı arasındaki ilişkinin incelenmesi*. Yüksek Lisans Tezi, Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Eğimli, A. T. (2009). Çalışanlarda iş doyumu: Kamu ve özel sektör çalışanlarının iş doyumuna yönelik bir araştırma. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 23(3), 35-52.
- Emek, S. (2006). *Sabit görüntüler ve video işaretleri için ayrık dalgacık dönüşümü ayrık kosinüs dönüşümü tabanlı sayısal damgalama yöntemi*. Doktora Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.
- Erbil, H. (2018). *Bilgi güvenliği stres faktörlerinin iş tatmininin üzerindeki etkileri: AR-GE merkezi olan işletmeler üzerine bir araştırma*. Yüksek Lisans Tezi, Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, Bursa.
- Ercan, C. (2009). İnternet kullanımında etik kaygılar ve etik kaygıların giderilmesi yönünde organizasyonların sorumlulukları. *Mevzuat Dergisi*, 11(141), 1-11.
- Eriksson, E. (2018). What is the role of a computer scientist in shaping a sustainable future? *XRDS: Crossroads, The ACM Magazine for Students*, 25(1), 48-51. Doi: <https://doi.org/10.1145/3265901>.
- Ermiş, Ü. (2018). Bir güvenlik sorunu olarak siber uzay.

- Erol, S. E., Ceyhan, E. B. ve Sağıroğlu, Ş. Kişisel, kurumsal ve ulusal bilgi güvenliği farkındalığı üzerine bir inceleme. 1-9.
- Ersoy, E. V. (2012). *ISO/IEC 27001 Bilgi Güvenliği Standardı*. Ankara: ODTÜ Yayıncılık.
- Eş. A ve Serdar, N. Siber saldırılara karşı kobilerin farkındalık düzeylerinin incelenmesi: Ankara ili örneği. *Düzce Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 11(1), 133-151.
- Fakeh, S. K., Zulhemay, M. N., Shahibi, M. S. ve Zaini, J. A. (2012). Information security awareness amongst academic librarians. *University Technology MARA*, 8(3), 1723-1735.
- Farooq, A. (2013). *Information security awareness assessment: a case of university of Turku*. Yüksek Lisans Tezi, Turku Üniversitesi Bilgi Teknolojileri Bölümü, Finlandiya.
- Fidan, Y. (2011). Özel sektör ve kamu yöneticilerinin zaman yönetimi davranışlarının karşılaştırılması. *Adıyaman Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 6, 47-74.
- Gazdağı, O. ve Çetinyokuş, T. (2020). Bankacılık sektöründe bilgi güvenliği ve iş sürekliliğinin sağlanması amacıyla ISO/IEC 27001 ve ISO 22301 standartlarının uygulanmasına yönelik kavramsal inceleme. *Journal of Humanities and Tourism Research*. 10(2),475-491.
- Gebru, M. M. (2020), Information security awareness of employees in Ethiopian banking sector. *North American Academic Research*.
Doi:<https://doi.org/10.5281/zenodo.4087125>.
- Gencer, K. (2015). *ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım*. Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon.
- Genç, S. Z. ve Eryaman, M. Y. (2008). Değişen değerler ve yeni eğitim paradigması. *Sosyal Bilimler Dergisi*, 9(1), 89-102.
- George, D. ve Mallery, P. (2019). *IBM SPSS Statistics 25 step by step: A Simple guide and reference* (Onbeşinci Baskı). Amerika: Routledge.
- Gibson, W. (1984). *Neuromancer*. (Çevirmen: Sengül Oğur). Türkiye: Altıkkırkbeş Basın Yayın.
- Gliem, J. A. and Gliem, R. R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. *Midwest Research-to-Practice Conference in Adult, Continuing and Community Education*, 82-88.
- Gonzalez, J. J. ve Sawicka, A. (2002, October). A framework for human factors in information security. In *Wseas international conference on information security, Rio de Janeiro*, 448-187.
- Goody, J. (2009). *Renaissances: the one or the many?* ABD: Cambridge University Press

Yayınevi, Cambridge.

Gök, M. S. (2012). *5651 Sayılı kanun ve bilgi güvenliği ilişkisi*. Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Gökçen, M. Y. ve Çetin, S. (2022). Yenilikçi İş Davranışının İş Performansına Etkisi. *Optimum Ekonomi ve Yönetim Bilimleri Dergisi*, 9(2), 174-188.

Gökçearslan, Ş. ve Günbatar, M. S. (2012). Ortaöğrenim öğrencilerinde internet bağımlılığı. *Eğitim Teknolojisi Kuram ve Uygulama*, 2(2), 10-24.

Gökçearslan, Ş., Günbatar, M. S. ve Sarıtepeci, M. (2021). Ortaöğretim öğrencilerinin bilgi güvenliği farkındalıklarının incelenmesi. *Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi*, 18(1), 354-373.

Gökçearslan, Ş., Nezgıtlı, S. ve Çakır, H. (2020). Bilişim suçu haberlerinin basında sunumu: 2009-2019 yılları arası çevrimiçi gazete haberleri örnekleme. *Bilgi ve İletişim Teknolojileri Dergisi*, 2(2), 149-160.

Göldağ, B. (2021). Üniversite öğrencilerinin dijital okuryazarlık düzeyleri ile dijital veri güvenliği farkındalık düzeyleri arasındaki ilişkinin incelenmesi. *e-Uluslararası Eğitim Araştırmaları Dergisi*, 12(3), 82-100.

Güldüren, C. (2015) *Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi*. Doktora Tezi, Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Gülmüş, M. (2010). *Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği*. Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Gülseçen, S. (2014). Bir değer olarak bilgi ve bilginin yönetimi. *Türk Kütüphaneciliği*, 28(1), 62-68.

Gündüz, M. Z. ve Daş, R. (2016). Sosyal Mühendislik: yaygın ataklar ve güvenlik önlemleri. *9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, 11-18.

Gündüz, M. Z. ve Daş, R. (2014). Kablosuz yerel alan ağlarına sızma uygulaması ve temel güvenlik önerileri. In *7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (7th International Conference on Information Security and Cryptology-ISCTURKEY 2014)*, 295-300.

Gündüzalp, C. (2021). Üniversite çalışanlarının dijital veri ve kişisel siber güvenlik farkındalıkları (Bilgi İşlem Daire Başkanlıkları örneği). *Journal of Computer and Education Research*, 9(18), 598-625.

Güngör, M. (2015). *Ulusal bilgi güvenliği: strateji ve kurumsal yapılanma*. Uzmanlık Tezi, TC Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı, Ankara.

Güngör, U. ve Güney, O. (2017). Uluslararası ilişkilerde güvenliğin dönüşümü çerçevesinde bilgi güvenliği ve siber savaş. *Journal of Excipients ve Food Chemicals*, XIV(55),

131-146.

Gürsel, T. (2019). *Sigorta şirketlerinde bilgi güvenliği yönetim sistemi denetimi*. Doktora Tezi, Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü, İstanbul.

Gürkaynak, M. ve İren, A. A. (2011). Reel dünyada sanal açmaz: Siber alanda uluslararası ilişkiler. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 16(2), 263-279.

Gürüz, E.D. ve Gürel Ş.E. (2006). Yönetim ve organizasyon: Bireyden örgüte, fikirden eyleme. Ankara: Nobel Yayın Dağıtım.

Gürz, U. (2019). İngiltere’de Sanayi Devrimi. *Academia*, 1-7.

Hadlington, L. ve Chivers, S. (2020). Segmentation analysis of susceptibility to cybercrime: exploring individual differences in information security awareness and personality factors. *Policing: A Journal of Policy and Practice*. 14(2), 479-492.

Haeussinger, F. ve Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior.

Hagen, J. M. ve Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management ve Computer Security*.

Hardy, I. R. (1996). The evolution of ARPANET email. Tarih Tezi, California Üniversitesi Tarih Bölümü, California.

Henkoğlu, T. (2020). *Adli bilişim: Dijital delillerin elde edilmesi ve analizi*. 2. Baskı, Pusula Yayıncılık.

Henkoğlu, T. ve Yılmaz, B. (2013). Avrupa Birliği AB bilgi güvenliği politikaları. *Türk Kütüphaneciliği*, 27(3), 451-471.

Hu, Q., Dinev, T., Hart, P. ve Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615-660.

Huck, S. W. (2012). *Reading statistics and research* (Altıncı Baskı). Amerika: Pearson.

Hutinski, K. ve Bamir, (2009). A method for analysis of corporate information security awareness. *The Proceedings of the 1st International Conference on Information Society and Information Technologies ISIT 2009*, 76-80.

Irmak, H. ve Reis, Z. A. (2018). A web-based awareness education against social engineering attacks, *PREFACE OF THE EDITORS*, 108.

İnternet: Adalet İstatistikler 2020. URL: https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/1692021162011adalet_ist-2020.pdf Son Erişim Tarihi: 29.07.2022.

İnternet: Adalet İstatistikler 2020. URL: <https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/310520221416422021H%C4%B0ZMETE%C3%96ZELK%C4%B0TAP.pdf> Son Erişim Tarihi: 29.07.2022.

İnternet: Association for Information Systems, International Conference on Information Systems. URL: <https://aisnet.org/page/ICISPage> Son Erişim Tarihi: 29.06.2021.

İnternet: Berksoy, M. Veri ve bilgi nedir? Arasındaki fark nedir? Neden önemlidir?. TeknoTower. URL: <https://teknotower.com/veri-ve-bilginin-onemi-1/>, Son Erişim Tarihi: 28.06.2021.

İnternet: Barry, Sean; “Smoking microchips tells it all: Computer forensic experts mine hard drives for data that too- clever users thought long deleted”. URL: http://www.dataforensics.com/articles/smoking_microchip_tells_it_all.pdf. Son erişim tarihi: 25.07.2022.

İnternet: BGA Güvenlik, Etkinlikler. URL: <https://www.bgasecurity.com/etkinlik/istsec19-istanbul-bilgi-guvenligi-konferansi/> Son Erişim Tarihi: 29.06.2021.

İnternet: Bilişim Ajandası (2011). 11 yıllık siber suç haritamız çıkarıldı. URL: <http://www.bilisimdergisi.org.tr/s137/pdf/14-19.pdf> Son Erişim Tarihi: 22.07.2022

İnternet: Cisco, 2009 Görsel Ağ İndeksi. URL: https://www.cisco.com/c/dam/global/pt_br/assets/docs/whitepaper_VNI_06_09.pdf Son Erişim Tarihi: 11.12.2021.

İnternet: Cisco, 2013 Görsel Ağ İndeksi. URL: <https://newsroom.cisco.com/press-release-content?type=webcontentvearticleId=1135354> Son Erişim Tarihi: 11.12.2021.

İnternet: Cisco, What Is Information Security. URL: <https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html> Son Erişim Tarihi: 20.01.2021.

İnternet, Cumhuriyet (2021). Siber güvenlik uzmanı yanıtladı: Akbank'ta 35 saattir neler oluyor?. URL: <https://www.cumhuriyet.com.tr/haber/siber-guvenlik-uzmani-yanitladi-akbankta-35-saattir-neler-oluyor-1850638> Son Erişim Tarihi: 20.07.2022.

İnternet, Dijital Dönüşüm Ofisi. URL: <https://cbddo.gov.tr/projeler/81ilde81siberkahraman/> Son Erişim Tarihi: 20.07.2022.

İnternet: Doğan, M., Bilgi güvenliğinde farkındalık ve insan faktörü. URL: <https://www.rskveri.com/bilgi-guvenliginde-farkindalik-ve-insan-faktoru/> Son Erişim Tarihi: 01.01.2022.

İnternet: Elektrik Mühendisleri Odası, 1.Ağ ve Bilgi Güvenliği Sempozyumu <http://abg.emo.org.tr/index.php?etkinlikkod=9>, Son Erişim Tarihi: 29.06.2021.

İnternet: FS-ISAC, Reducing cyber risk in the global financial sector. URL: <https://www.fsisac.com/what-we-do> Son Erişim Tarihi: 29.06.2021.

İnternet: HITB Security Conference, What is the HITBSECCONF?. URL:

<https://conference.hitb.org/> Son Erişim Tarihi: 29.06.2021.

İnternet: Honeypot, 2018 Women in Tech Index. URL: <https://honeypotio.github.io/women-in-tech/> Son Erişim Tarihi: 06.12.2021.

İnternet: Hosting Blog, Bulut Teknolojisi Nedir?. URL: <https://www.hosting.com.tr/blog/php-vs-asp-farki-avantaji/> Son Erişim Tarihi: 03.01.2022.

İnternet: InfoSecurity Europe. <https://www.infosecurityeurope.com/> Son Erişim Tarihi: 29.06.2021.

İnternet: International Telecommunications Union (ITU). Cyber Security Guide For Developing Countries 2007. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007-PDF-E.pdf Son Erişim Tarihi: 29.06.2021.

İnternet: International Telecommunications Union (ITU). ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity 2008. URL: https://www.gp-digital.org/wp-content/uploads/2018/08/ITU_Explainers_cybersecurity.pdf. Son Erişim Tarihi: 28.06.2021.

İnternet: ISC Turkey. URL: <https://isc-turkey.org/gecmis-konferanslar/> Son Erişim Tarihi: 29.06.2021.

İnternet: ISO, ISO/IEC 27001 Information Security Management. URL: <https://www.iso.org/isoiec-27001-information-security.html> Son Erişim Tarihi: 04.12.2021.

İnternet: ISO, ISO/IEC 27001:2013 Information Technology, Security Techniques, Information Security Management Systems, Requirements. URL: <https://www.iso.org/standard/54534.html> Son Erişim Tarihi: 21.01.2021.

İnternet: ITU, Veri ve bilgi nedir? Arasındaki fark nedir? Neden önemlidir?. TeknoTower. URL: <https://teknotower.com/veri-ve-bilginin-onemi-1/>, Son Erişim Tarihi: 28.06.2021.

İnternet: Koca, E. Bilgisayar Ağları; Bilgisayar İletişimi Nedir? Veri İşleme Modelleri ve Ağ Gelişimi Merkezi İşleme. URL: <https://docplayer.biz.tr/5979019-Bilgisayar-aglari-bilgisayar-iletisimi-nedir-veri-isleme-modelleri-ve-ag-gelisimi-merkezi-isleme.html> Son erişim tarihi: 05.01.2022.

İnternet: Milli Kütüphane, Dijital Kütüphane Hizmetleri. URL: <https://dijital-kutuphane.mkutup.gov.tr/>, Son Erişim Tarihi: 29.06.2021.

İnternet: Osterman Resarch, 2020 State of Privacy and Security Awareness Report. URL: https://www.bsigroup.com/globalassets/localfiles/en-ie/our-services/mediapro/2020_state_of_privacy-security_awareness_report_mediapro.pdf Son erişim tarihi: 03.01.2022.

İnternet: OWASP, What is the OWASP foundation?. URL: <https://owasp.org/> Son Erişim Tarihi: 29.06.2021.

İnternet: SANS, 2021 Security Awareness Report. URL: <https://www.sans.org/security-awareness-training/resources/reports/sareport-2021/> Son Erişim Tarihi: 03.01.2022.

İnternet: Springer Link, International Conference on Information Security. URL: <https://link.springer.com/conference/isw> Son Erişim Tarihi: 29.06.2021.

İnternet: TKDK, Bilgi Güvenliği Nedir. URL: <https://www.tkd.gov.tr/Kurumsal/BGYs#:~:text=Bilgi%20g%C3%BCvenli%C4%9Fi%2C%20bilginin%20izinsiz%20veya,%C3%BC%C3%A7%20temel%20unsurdan%20meydana%20gelir> Son Erişim Tarihi: 19.01.2021

İnternet: TÜBİSAD, 2018 Teknoloji sektöründe kadın. URL: <https://www.tubisad.org.tr/tr/images/pdf/deloitte-tubisad-teknoloji-sektorunde-kadin-raporu.pdf> Son Erişim Tarihi: 20.03.2022.

İnternet: TÜİK, 2021 İstatistiklerle Kadın. URL: <https://data.tuik.gov.tr/Bulten/Index?p=Istatistiklerle-Kadin-2021-45635> Son Erişim Tarihi: 21.03.2022.

Jagatic, T. N., Johnson, N. A., Jakobsson, M. ve Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94-100.

Jansson, K. ve von Solms, R. (2013). Phishing for phishing awareness. *Behaviour ve Information Technology*, 32(6), 584-593.

Jeimy, J. and Cano, M. (2019). The human factor in information security. *ISACA Journal*, 5, 1-7.

Jian-chuan, F., Guo-xiang, Z. ve Xin, Y. (2009). The Security technology and prevention measures to the spy software. *Journal of Anhui Vocational College of Electronics ve Information Technology*.

Johnson, M. E. ve Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy*, 5(3), 16-24.

Jondeau, E. ve Rockinger, M. (2003). Conditional volatility, skewness, and kurtosis: existence, persistence, and comovements. *Journal of Economic Dynamics ve Control*, 27, 1699– 1737.

Kalman, S. (2003). *Web security field guide*. Cisco Press. Indianapolis.

Kara, O. ve Topaloğlu, M. (2019). Bilgisayar teknolojileri ve bilişim sistemleri öğrencilerinin bilişim güvenliği alanında yeterliliklerinin incelenmesi. *Ege Eğitim Teknolojileri Dergisi*, 3(1), 20-27.

Karaarslan, E. (2003). Ağ güvenlik duvarı çözümü oluşturulurken dikkat edilmesi gereken hususlar. *Akademik Bilişim*.

- Karaarslan, E., Teke, A. ve Şengonca, H. (2003). Bilgisayar ağlarında güvenlik politikalarının uygulanması. *V. Akademik Bilişim Konferansı*.
- Karabatak, S. ve Karabatak, M. (2019). Information security awareness of school administrators. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*. Doi: 10.1109/ISDFS.2019.8757525.
- Karadağ, Ş. (2019). *Siber uzayın NATO'nun güvenlik anlayışına etkisi*. Yüksek Lisans Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.
- Karadağ, M. ve Abuhanoğlu, H. (2015). Sosyo-kültürel özelliklerin bilgi güvenliği farkındalığı üzerine etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesinde bir çalışma. *The Journal of Academic Social Science Studies*, (36), 379-386
- Karakuş, S., (2018). *Derin öğrenme yöntemlerinin kullanılarak dijital deliller üzerinde adli bilişim incelemesi*. Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ.
- Karaoğlu, Yılmaz, F. G., Yılmaz, R. ve Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi*, 3(1), 176-199.
- Karasar, N. (2012). *Bilimsel araştırma yöntemleri* (Yirmidördüncü baskı). Türkiye: Nobel Yayınevi.
- Karasar, N. (2020). *Bilimsel araştırma yöntemi* (Otuzbeşinci Baskı). Türkiye: Nobel Yayınevi.
- Kaur, J. ve Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. *In 2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 286-290.
- Kavurucu, Y. ve Sever, Ö. (2016). Hybrid non-repudiation protocol with all types of pairings. *Journal of Naval Sciences and Engineering*, 12(1), 33-50.
- Kaya, Ö. F. (2017). *Kurumsal işletmelerde bilgi ve veri güvenliği*. Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.
- Kazan, S. ve Vural, C. (2016). Sayısal görüntü damgalama yöntemlerinin Jpeg sıkıştırmasına karşı dayanıklılığının karşılaştırılması. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, 2(1).
- Kenning, M. J. (2001). Security management standard ISO 17799/BS 7799. *BT Technology Journal*, 19(3), 132-136.
- Keser, H. ve Yayla, H. G. (2021). FATİH Projesi uygulanan okullardaki öğretmenlerin bilgi güvenliği farkındalık düzeylerinin incelenmesi. *Milli Eğitim Dergisi*, 50(229), 9-40.
- Keskin, D. A. ve Gözenman, S. (2019). Hile riski açısından sosyal mühendislik. *TİDE Academia Research*, 1(2), 281-306.

- Khan, B., Alghathbar, K. S., Nabi, S. I., and Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African journal of business management*, 5(26), 10862-10868.
- Khan, W. Z., Aalsalem, M. Y., and Xiang, Y. (2011). A graphical password based system for small mobile devices. *IJCSI International Journal of Computer Science Issues*, 8(5), 145-154.
- Kjørvik, H. (2010). *Implementing and improving awareness in information security*. Yüksek Lisans Tezi, Agder Üniversitesi, Norveç.
- Kılıçaslan, S. (2010). *Örgütsel adalet algısı ve örgütsel bağlılık arasındaki ilişkilere kuramsal bir yaklaşım*. Yüksek Lisans Tezi Dokuz Eylül Üniversitesi Sosyal Bilimleri Enstitüsü, İzmir.
- Kocacık, F. (2003). Bilgi toplumu ve Türkiye. *CÜ Sosyal Bilimler Dergisi*, 27(1), 1-10.
- Koçak, H. ve Memiş, K. (2018). Bilgi toplumunda korku: bilgi güvenliği ve risk toplumu. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*, 20(3), 1-10.
- Konacaklı, E. (2019). *Ulusal güvenlik için blokzinciri tabanlısiber güvenlik modeli*, Yüksek Lisans Tezi, Eskişehir Teknik Üniversitesi Fen Bilimleri Enstitüsü, Eskişehir.
- Köktürk, E. ve Avcı, Ü. (2019). Kurumsal bilgi güvenliği farkındalığı üzerine bir çalışma. *7th International Instructional Technologies and Teacher Education Symposium ITTES 2019 Abstract Book*.
- Kraus, A. (2018). *Developing an information security strategy*. Yüksek Lisans Tezi, St Pölten Üniversitesi, Avusturya.
- Kruger, H. A. and Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers ve security*, 25(4), 289-296.
- Kruger, H., Drevin, L., and Steyn, T. (2010) A vocabulary test to assess information security awareness. *Information Management and Computer Security*. 18(5), 316-327.
- Kulakoğlu, D. (2013). *KOBİ'lerde yönetim ve organizasyon sorunlarının yaşanma düzeyi: Ankara KOBİ örneği*. Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Kurnaz, N. ve Dindaroğlu, A. K. (2016). İç denetim ve bilgi güvenliği ilişkisi: Bölgesel bir araştırma. *Bilgi Ekonomisi ve Yönetimi Dergisi*, 10(1).
- Kurt, S. G. (2019). *Bilgi güvenliğinin bilgi işlem çalışanları tarafından değerlendirilmesi sağlık sektöründe bir çalışma*. Doktora Tezi, Marmara Üniversitesi Sağlık Bilimleri Enstitüsü, İstanbul.
- Lim, J. S., Chang, S., Maynard, S. ve Ahmad, A. (2009). Exploring the relationship between organizational culture and information security culture.
- Marcinkowski, S. J. and Stanton, J. M. (2003). Motivational aspects of information security

- policies. In *SMC'03 Conference Proceedings*, 3, 2527-2532.
- Marşap, A., Akalp, G., ve Yeniman, E. (2010). Sağlık işletmelerinde insan kaynağının kurumsal bilgi güvenliği kültürü gelişimi. *Bilişim Teknolojileri Dergisi*, 3(1), 31-40.
- Mart (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı*. Yüksek Lisans Tezi, Kahramanmaraş Sütçü İmam Üniversitesi Fen Bilimler Enstitüsü, Kahramanmaraş.
- Maynard, S., Ruighaver, A. ve Chia, P. (2002). Exploring organisational security culture: Developing a comprehensive research model. *In Proceedings*.
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. ve Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151-156.
- McCumber, J. (1991). Information systems security: A comprehensive model. *In Proceedings 14th National Computer Security Conference*, 328-337.
- Mears, L. ve Von Solms, R. (2004). Corporate information security governance: a holistic approach. *ISSA*.
- Mellor, M. ve Noyes, D. (2007). Awareness and accountability in information security training. *In 6th Annual Security conference The Information Institute*.
- Meral, S. ve Bülbül, H. İ. (2022). Kamu kurumlarının bilgi güvenliği politikalarının kurumsal bilgi güvenliğinin sağlanması açısından etkinliğinin analiz edilmesi. *Gazi University Journal of Science Part C: Design and Technology*, 10(2), 314-329.
- Mete, H. (2010). *ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin bilgi işlem merkezlerinde uygulanması*. Yüksek Lisans Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya.
- Mitchell, R. C., Marcella, R. ve Baxter, G. (1999). Corporate information security management. *New Library World*, 100(5), 213-277.
- Nezgitli, S. (2021), *İngiltere ve Türkiye'nin siber güvenlik politikalarının karşılaştırılması*. Uzmanlık Tezi, Radyo ve Televizyon Üst Kurulu Strateji Geliştirme Dairesi Başkanlığı, Ankara.
- Oğuz, S., Ceyhan, E. B. ve Sağıroğlu, Ş. (2015). Teknolojinin casuslukta kullanılması ve karşı önlemler. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISC Turkey)*, 1-6. 2
- 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*, 1-15, Niğde.
- Okul, T., Şimşek, G., Hafçı, B., ve Barış, Z. (2018). Bilgi güvenliği farkındalığı: Kuşadası'ndaki konaklama işletmesi yöneticileri üzerine bir uygulama. *Uluslararası Türk Dünyası Turizm Araştırmaları Dergisi*, 3(2), 189-201.

- Oudkerk, S., Bryant, I., Eggen, A., and Haakseth, R. (2010). A proposal for an XML confidentiality label and related binding of metadata to data objects. *NATO C3 Agency The Hague*.
- Öğütçü, G., Testik, Ö. M., ve Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers ve Security*, 56, 83-93.
- Önder, T. (2014). *Kamu ve özel sektör yöneticilerinin yönetsel narsizm düzeylerinin karşılaştırılması*, Yüksek Lisans Tezi, Maltepe Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Özaslan, G. (2019). *Bilgi güvenliği ve mahremiyetin korunmasına yönelik eğitimin etkilerinin değerlendirilmesi: Bir özel hastane uygulaması*. Yüksek Lisans Tezi, Marmara Üniversitesi Sağlık Bilimleri Enstitüsü, İstanbul.
- Özdemir, A. (2019). *Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı*. Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara.
- Özdemir, A. ve Uluyol, Ç. (2021) Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, 25(3), 649-666.
- Özdemir, S., Kalkan, Ö. K., Türkoğlu, A., Varol, N. ve Tokdemir, M. (2013). Elazığ'da üniversite ve lisede öğrenim gören bilgisayar bölümü öğrencilerinin adli bilişim suçlarına yaklaşımları. *Medical Sciences*, 8(3), 16-25.
- Özden Aktaş, F., Karabağ, R., Uğur, A., Akyüz, T., Takçı, H. ve Soğukpınar, İ. (2020). Bilgi güvenliği politikasının uygulama başarısını artırmak için yeni bir yaklaşım. *ELECO 2008 Bildirisi*.
- Özgeldi Büyüktopbaş, H. (2016). *Endüstri ürünlerinde bilgilendirme tasarımı ve iletişim sorunları*. Yüksek Lisans Tezi, Işık Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Özkaya, M. O. ve Şengül, C. M. (2006). İş etiği örnek olaylarla kurumlar ve cinsiyetler arasındaki tepkisel farklılıklar. *Yönetim ve Ekonomi Araştırmaları Dergisi*, 4(6), 70-87.
- Özsoy, O. (2014). *İktisatçılar ve işletmeciler için istatistik excel uygulamalı* (Dördüncü Baskı). Türkiye: Siyasal Kitapevi.
- Öztemiz, S. ve Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği (Awareness of information security in information centers: sample of academic libraries in Ankara). *Bilgi Dünyası*, 14(1), 87-100.
- Öztezcan, B. A. ve Çetinkaya, A (2017). Bilgi güvenliği farkındalığı üzerine bir araştırma: Marmara Üniversitesi örneği. *Ulusal Multidisipliner Hakemli Sosyal Bilimler ve Araştırma Dergisi*, 56-71.
- Öztürk, İ. ve Çakır, R. Öğretmenlerin sınıf ortamında dijital oyunlardan yararlanmaları ve dijital veri güvenliği farkındalıkları. *Türkiye Bilimsel Araştırmalar Dergisi*, 7(1), 123-

146.

- Paloque Berges, C. ve Schafer, V. (2019). Arpanet (1969–2019). *Internet Histories*, 3(1), 1-14.
- Papadaki, M. ve Furnell, S. (2004). IDS or IPS: what is best? *Network Security*, 2004(7), 15-19.
- Parlak, A. (2005). *İnternet ve Türkiye’de internetin gelişimi*. Bitirme Ödevi, Fırat Üniversitesi Mühendislik Fakültesi, Elazığ.
- Parlakkılıç, A. ve Uysal, M. P. (2010) E-Öğrenme sistemlerinde güvenlik tehditleri ve karşı tedbirler. *10th International Educational Technology Conference*, 527-532.
- Parker, D. B. (1968). Rules of ethics in information processing. *Communications of the ACM*, 11(3), 198-201.
- Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. ve Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management ve Computer Security*, 22(4), 334-345.
- Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D. ve McCormac, A. (2019). Matching training to individual learning styles improves information security awareness. *Information and Computer Security*.
- Pattinson, M., Butavicius, M., Parsons, K., McCormac, A. ve Calic, D. (2017). Managing information security awareness at an Australian bank: A comparative study. *Information ve Computer Security*.
- Pfleeger, S. L., Sasse, M. A. ve Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, 11(4), 489-510.
- Polat, D. (2020). NATO’nun yeni operasyon alanı: Siber uzay. *Güvenlik Bilimleri Dergisi*, 135-158.
- Polic, V. D. (2012). Implementing audit ability with non interactive zero knowledge proofs. *Metalurgia International*, 17(11), 106.
- Reid, R. ve Niekerk, J. V. (2014). From information security to cyber security cultures. *IEEE Conference Publications 2014 Information Security for South Africa*, 1-7.
- Rençber, Ö. F. ve Mete, S. (2017). Bilgi güvenlik farkındalığını etkileyen faktörlerin belirlenmesi: yüksekokul öğrencileri üzerine bir inceleme. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 18(3), 800-823.
- Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, 2(3), 1-28.
- Röhrig, S. (2003). *Using process models to analyse it security requirements*. Doktora Tezi,

Zürich Üniversitesi, Almanya.

Sağıroğlu, Ş. ve Karaman, M. (2012). Adli Bilişim. *Telepati Haberleşme ve Bilişim Teknolojileri Dergisi*, 203(67).

Samonas, S., ve Coss, D. (2014). The CIA strikes back: redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, 10(3), 21-45.

Sasse, M. A., Brostoff, S., and Weirich, D. (2001). Transforming the ‘weakest link’ a human/computer interaction approach to usable and effective security. *BT technology journal*, 19(3), 122-131.

Savolainen, P., Niemela, E. ve Savola, R. (2007). A taxonomy of information security for service centric systems. *In 33rd EUROMICRO Conference on Software Engineering and Advanced Applications*. 5-12.

Say, M. ve Sağıroğlu, Ş. (2004). Bilgisayar veri güvenliği üzerine bir inceleme: klavye dinleme sistemleri.

Schlienger, T. and Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. *In 14th International Workshop on Database and Expert Systems Applications*. 405-409.

Semiz, K. ve Tüfekçi, A. (2019). Kurumsal bilgi yönetim modelleri süreçlerinin analizi ve karşılaştırılması. *7th International Instructional Technologies and Teacher Education Symposium ITTES 2019 Abstract Book*.

Sevgi, S. ve Yakışıklı, Z. (2020). Ortaokul öğrencilerinin matematik öz-yeterlik algılarının ve matematiğe yönelik tutumlarının incelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, 16(2), 394-416.

Shakarian, P., Shakarian, J. ve Ruef, A. (2013). Attacking iranian nuclear facilities: Stuxnet. *Introduction to cyber-warfare: A multidisciplinary approach*, 223-239.

Shaw, R. S., Chen, C. C., Harris, A. L. ve Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers ve Education*, 52(1), 92-100. 92

Shehri, Y. ve Clarke, N. L. (2007). Information security awareness and culture. P. Dowland, ve S. Furnell (Eds.). *Advances in Networks, Computing and Communications*, 6, 12-22.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, 8(1), 31-41.

Solomon, M. ve Chapple, M. (2005). *Information security illuminated*. Canada: Jones and Bartlett Publishers.

Solmaz, M. (2020). Öğretmen adaylarının siber bilgi güvenliği farkındalıklarının ve dijital vatandaşlık düzeylerinin farklı değişkenler açısından incelenmesi. Yüksek Lisans Tezi, Mersin Üniversitesi Eğitim Bilimleri Enstitüsü, Mersin.

- Stephanou, A. (2008). *The impact of information security awareness training on information security behaviour*. Araştırma Raporu, Witwatersrand Üniveristesi, Ticaret, Hukuk ve İşletme Fakültesi, Güney Afrika.
- Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim*, 9, 11-13.
- Tabachnick, B. G. Fidell, L. S. ve Ullman, J. B. (2007). *Using Multivariate Statistics*, (Beşinci Baskı). ABD: Pearson.
- Taherdoost, H., Chaeikar, S., Jafari, M. ve Shojae Chaei Kar, N. (2013). Definitions and criteria of CIA security triangle in electronic voting system. *International Journal of Advanced Computer Science and Information Technology (IJACSIT)*, 1, 14-24.
- Tamjidyamcholo, A., Baba, M. S. B., Tamjid, H. ve Gholipour, R. (2013). Information security: Professional perceptions of knowledge sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers and Education*, 68, 223-232.
- Talan, T. ve Aktürk, C. (2021). Orta öğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, 18(1), 158-180.
- Taner, E. (2018). *Güvenlik güçlerinin bilgi güvenliği farkındalığına yönelik bir betimleme*. Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi, Fen Bilimleri Enstitüsü.
- Taner, E. ve Kılıç, İ. (2019). Güvenlik güçlerinin bilgi güvenliği farkındalığını belirlemeye yönelik bir araştırma. *Güvenlik Bilimleri Dergisi*, 8(2), 253-269.
- Teker, E. (2019). *Öğretmenlerin ve lise öğrencilerinin bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi*. Yüksek Lisans Tezi, Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Tekerek, M. (2008). Bilgi güvenliği yönetimi. *KSÜ Doğa Bilimleri Dergisi*, 11(1), 132-137.
- Thomson, K. L., Von Solms, R. ve Louw, L. (2006). Cultivating an organizational information security culture. *Computer fraud ve security*. 2006(10), 7-11.
- Topçu, N. (2020). Bir siber güç olarak Çin'in Siber Güvenlik Stratejisi. *Cyberpolitik Journal*, 5(10), 219-239.
- Tschakert, K. F. ve Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, 5(6), e02010.
- Tsohou, A., Karyda, M. ve Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers and security*, 52, 128-141.
- Tuluk, A. ve Seferoğlu, S. S. (2016). Ulusal ve uluslararası bilgi güvenliği politikalarının analizi üzerine karşılaştırmalı bir inceleme. *Uluslararası Eğitim Teknolojilerinde Yeni Eğilimler Konferansı INTET 2016*, 3-4.

- Türk Dil Kurumu (2005), *Türkçe Sözlük* (Onuncu Baskı). Türkiye: 4. Akşam Sanat Okulu Matbaası.
- Türkiye Bilişim Derneği, (2006). Bilişim Sistemleri Güvenliği El Kitabı Sürüm 1.0, *Türkiye Bilişim Derneği Yayınları*, Ankara.
- Uğur, A. ve Soğukpınar, İ. (2014). Kurumsal iş akışında sürdürülebilir yetki denetimi ve yetkili sayısal imza modeli. *Journal of the Faculty of Engineering and Architecture of Gazi University*, 29(3), 559-568.
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi*. UDHB, Ankara.
- Ulusal Siber Olaylara Müdahale Merkezi (2014), *Siber Güvenliğe İlişkin Temel Bilgiler*. USOM, Ankara.
- Utku, A. ve Doğru, İ. A. (2017). Android kötücül yazılımlar için izin tabanlı tespit sistemi. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 32(4), 1015-1024.
- Uzunsakal, E. ve Yıldız, D. (2018). Alan araştırmalarında güvenilirlik testlerinin karşılaştırılması ve tarımsal veriler üzerine bir uygulama. *Uygulamalı Sosyal Bilimler Dergisi*, 2(1), 14-28.
- Ünal, A. N. ve Ergen, A. (2018). Siber uzayda yeterince güvenli davranıyor muyuz? istanbul ilinde yürütülen nicel bir araştırma. *Manisa Celal Bayar Üniversitesi Sosyal Bilimler Dergisi*, 16(2), 191-216.
- Ünal, A. N. ve Yarman, B. S. B. (2014). Millî güç unsurlarının belirlenmesinde siber uzay faktörü. *7th International Conference On Information Security and Cryptology Proceedings Book*, 278-284.
- Van Niekerk, J. ve Von Solms, R. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. In *Issa*. 1(13).
- Varlı, B. ve Uluçınar Sağır, Ş. (2019). Araştırma sorgulamaya dayalı öğretimin ortaokul öğrencilerinin fen başarısı, sorgulama algısı ve üst biliş farkındalığına etkisi. *Gazi University Journal of Gazi Educational Faculty (GUJGEF)*, 39(2), 703-725.
- Varol, C., Cooper, P.A. ve Varol, A. (2013). Türkiye’de adli bilişim eğitimi. *1st International Symposium on Digital Forensics and Security (ISDFS’13)*, Elazığ.
- Veseli, I. (2011). Measuring the effectiveness of information security awareness program. Yüksek Lisans Tezi, Gjøvik Üniversitesi Bilgisayar Bilimi ve Medya Teknolojisi Bölümü, Norveç.
- Von Solms, B. (2001). Information security—a multidimensional discipline. *Computers ve security*, 20(6), 504-508.
- Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma testleri*. Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 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. 508.
- Wachira, J. K. (2021). *Factors affecting information security in teleworking case study: Kkenya national police dt sacco*. Doktora Tezi, Nairobi Üniversitesi Bilgisayar ve Bilişim Okulu, Kenya.
- Whitman, M. E., ve Mattord, H. J. (2021). *Principles of information security*. Cengage learning.
- Yan, Y., Qian, Y., Sharif, H., and Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys and Tutorials*, 14(4), 998-1010.
- Yavan, Ö. (2016). Örgütsel davranış düzleminde adanmışlık. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (25), 278-296.
- Yavuz, E. (2011). Kamu ve özel sektör çalışanlarının örgütsel adalet algılamaları üzerine bir karşılaştırma çalışması. *Doğuş Üniversitesi Dergisi*, 11(2), 302-312.
- Yavuz, H. ve Ulaş, M. (2013). Adli bilişime konu olan bilişim suçları ve bilgi güvenliği farkındalık tespiti. 1. In *International Symposium on Digital Forensics and Security Proceeding Book*.
- Yayla, H. G. (2018). *FATİH Projesi uygulanan ve uygulanmayan okullardaki öğretmenlerin bilgi güvenliği farkındalıklarının incelenmesi*. Yüksek lisans tezi, Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Yazıcı, N. (2021). *Türk Ceza Hukukunda bilişim suçları (TCK. M. 243-244 ve 245)*. Yüksek Lisans Tezi, Fatih Sultan Mehmet Vakıf Üniversitesi, Lisansüstü Eğitim Enstitüsü.
- Yerlikaya, T., Buluş, E. ve Buluş, N. (2006). Kripto algoritmalarının gelişimi ve önemi. *Akademik Bilişim Konferansları*, 9-11.
- Yıldırım, H. (2006). *Bankalarda operasyonel risk yönetimi ve bir uygulama*. Doktora tezi, Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü, İstanbul.
- Yılmaz, S. ve Salcan, O. (2008). *Siber Uzay'da Güvenlik ve Türkiye*. Türkiye: Milenyum Yayınları.
- Yılmaz, E., Şahin, Y. L. ve Akbulut, Y. (2015). Dijital veri güvenliği farkındalığı ölçeğinin geliştirilmesi. *AJIT-e: Bilişim Teknolojileri Online Dergisi*, 6(21), 23-40.
- Yılmaz, H. (2014). TS ISO/IEC 27001 Bilgi güvenliği yönetimi standardı kapsamında bilgi güvenliği yönetim sisteminin kurulması ve bilgi güvenliği risk analizi. *Denetçim*, 15, 45-59.
- Yılmaz, O. (2017). Küreselleşme sürecinde dönüşen güvenlik algısı ve siber güvenlik. *Cyberpolitik Journal*, 2(4), 22-43.

- Yüksel, F. (2005). Bilgi teknolojileri ve yerel yönetimler. *Sosyal Ekonomik Araştırmalar Dergisi*, 5(10), 246-259.
- Zhu, J., Zou, K., Liu, X. ve Gao, K. (2020). Establishment of response evaluation model and empirical study of risk in enterprise threat intelligence. *In 2020 2nd International Conference on Economic Management and Model Engineering (ICEMME)*. 735-738.





EKLER

EK-1. Kişisel Bilgi Formu

Değerli Katılımcı,

Bu anket çalışması, Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Ana Bilim Dalında Doç. Dr. Şahin GÖKÇEARSLAN danışmanlığında, Sena NEZGİTLİ tarafından hazırlanmakta olan **“Kamu Kurumu ve Özel Sektöre Yönelik Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme”** adlı yüksek lisans tezine veri temin edilmek amacıyla yapılmaktadır. Bu tezin bilime katkısı aşağıda sunulan anketin tamamlanması sayesinde olacaktır. Bu anket ile toplanacak veriler sadece bilimsel amaç için kullanılacak olup çalışmanın başarıya ulaşabilmesi sizlerin düşüncelerinizi doğru olarak aktarabilmesine bağlıdır. Katılımınızdan dolayı şimdiden teşekkür ederiz. Lütfen her bir soru için verilen seçeneklerin sadece birinin işaretleyiniz.

Doç. Dr. Şahin GÖKÇEARSLAN

Sena NEZGİTLİ

Gazi Üniversitesi

Gazi Üniversitesi

Uzaktan Eğitim Uygulama ve Araştırma Merkezi

BE Yüksek Lisans Öğrencisi

EK-1 (devam). Kişisel Bilgi Formu

Cinsiyetiniz nedir?	☐ Kadın ☐ Erkek
Çalıştığınız kurum türü nedir?	☐ Kamu kurumu ☐ Özel sektör
Hangi yaş aralığındasınız?	☐ 20-29 yaş arası ☐ 30-39 yaş arası ☐ 40-49 yaş arası ☐ 50 ve üzeri
Öğrenim durumunuz nedir?	☐ Lise ☐ Ön Lisans ☐ Lisans ☐ Yüksek Lisans ☐ Doktora
Çalıştığınız firmadaki/kurumdaki pozisyonunuz nedir?	☐ Yönetici ☐ Teknik personel ☐ İdari personel
Firmanızda/Kurumunuzda bilgi güvenliği farkındalığı hakkında eğitim/kurs veriliyor mu?	☐ Evet ☐ Hayır
Firmanızda/Kurumunuzda bilgi güvenliği farkındalığı üzerine ne sıklıkla eğitim/kurs veriliyor?	☐ Üç ayda bir ☐ Altı ayda bir ☐ Yılda bir ☐ Bir yıldan fazla
Firmanızda/Kurumunuzda verilen bilgi güvenliği farkındalığı eğitimleri/kursları ne kadar faydalı?	☐ Çok faydalı ☐ Faydalı ☐ Karasızım ☐ Faydasız
Firmanızda/Kurumunuzda bilgi güvenliği politikası mevcut mu?	☐ Evet ☐ Hayır
Firmanızda/Kurumunuzda bilgi güvenliği politikasının uygulanma derecesi nedir?	☐ Oldukça uygulanıyor ☐ Uygulanıyor ☐ Uygulanmıyor ☐ Hiç uygulanmıyor

EK-2. Bilgi Güvenliği Farkındalığı Ölçeği

<i>Lütfen, her bir ifadeye ilişkin katılım düzeyinizi belirtiniz.</i> 1-Kesinlikle Katılmıyorum 2-Katılmıyorum 3-Kararsızım 4-Katılıyorum 5.Kesinlikle Katılıyorum	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1. Firmamız, yetkimizin olmadığı dosyalara girişlerimizi engeller.(Raporlar, Sistem dosyası, Bilgi deposu, Ortak dosya vs.)	(1)	(2)	(3)	(4)	(5)
2. Firmamızda, teknolojik cihazlarda (makina, bilgisayar ve benzeri) izinsiz erişimi engellemek adına gerekli önlemler bulunur.	(1)	(2)	(3)	(4)	(5)
3. Firmamızda, önemli bilgilerin gizliliğinin korunabilmesi için ‘‘Güvenli belge deposuna benzer önlemler bulunur.(Bilgi Deposu vs.)	(1)	(2)	(3)	(4)	(5)
4. Firmamızda, önemli bilgilerin gizliliğinin korunabilmesi için ‘‘Genel güvenlik politikaları’’ uygulanır.	(1)	(2)	(3)	(4)	(5)
5. Firmamızda, önemli bilgilerin gizliliğini korunabilmesi için ‘‘Bilgi saklama alanı’’ kullanılır.(Sistem Dosyası, Bilgi dosyası, vs.)	(1)	(2)	(3)	(4)	(5)
6. Firmamız, önemli bilgilerin gizliliğinin korunabilmesi için ‘‘son kullanıcıların eğitimine ‘‘ önem verilir.	(1)	(2)	(3)	(4)	(5)
7. Firmamızda, önemli bilgilerin gizliliğinin korunabilmesi için ‘‘Bilgi sınıflandırması’’ kullanılır.(İhracat Departmanı, İthalat Departmanı, İç piyasa)	(1)	(2)	(3)	(4)	(5)
8. Firmamız, internetten yüklenen bütün dosyaların virüs programıyla taranmasına önem gösterir.	(1)	(2)	(3)	(4)	(5)
9. Firmamız, müşterilerimizle olan iletişim sırasında herhangi bir verinin değiştirilmesi olasılığına karşı önlem alınır.	(1)	(2)	(3)	(4)	(5)
10. Ciddi bir siber saldırı ile bilgilerimizin zarar görmesi durumunda firmamızın önemli derecede etkileneceğini düşünmekteyim.	(1)	(2)	(3)	(4)	(5)
11. Firmamızda, verilerin izinsiz değiştirilmesi konusunda önlemler alınır.	(1)	(2)	(3)	(4)	(5)

EK-2 (devam). Bilgi Güvenliği Farkındalığı Ölçeği

12. Kullandığımız bilişim sistemlerinin herhangi bir unsurunun (yazılım veya donanım vb.) kendisinden beklenildiği şekilde çalışmaması işlerimizi önemli ölçüde yavaşlatır	(1)	(2)	(3)	(4)	(5)
13. Firmamız, mail aracılığıyla gelebilecek olan virüslerin sistemimize girmemesi için önlemler alır.	(1)	(2)	(3)	(4)	(5)
14. Firmamız, bilgisayarımıza casus yazılım yüklenmesini engellemek için önlem alır.	(1)	(2)	(3)	(4)	(5)
15. Firmamız, dosya erişimlerine ulaşma hızımız yavaşladığında önlem alır.	(1)	(2)	(3)	(4)	(5)
16. Firmamızın, mail aracılığıyla zararlı dosyaların sistemimize girmemesi için önlemleri göz ardı eder.	(1)	(2)	(3)	(4)	(5)
17. Firmamızda evrakların imha işlemi verinin izlenebilirliğini azaltmak için kullanılır.	(1)	(2)	(3)	(4)	(5)
18. Firmamızda, önemli evrakların değiştirilme ihtimaline karşı önlem alır.	(1)	(2)	(3)	(4)	(5)
19. Firmamızda, bilgi sistemlerine ‘‘üçüncü taraf’’ (dışarıdan) erişim, üst düzey bir yöneticinin onayını gerektirir.	(1)	(2)	(3)	(4)	(5)
20. Firmamız verilerin kopyalanmasını engeller.	(1)	(2)	(3)	(4)	(5)
21. Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.	(1)	(2)	(3)	(4)	(5)
22. Firmamız, sistemdeki arızanın kaynağını tarihsel kayıtlardan çıkartabilir.	(1)	(2)	(3)	(4)	(5)
23. Firmamız, dosya ya da önemli bir evrak değiştirildiği zaman, değişiklik yapan kullanıcıyı görebilir.	(1)	(2)	(3)	(4)	(5)
24. Firmamız, sistemde değişikliklerden dolayı doğabilecek sorunları engellemek için önlemler alır.	(1)	(2)	(3)	(4)	(5)
25. Firmamız, siber güvenlik açısından olası riskler olabileceğini düşünür ve bunlara karşı önlemler alır.	(1)	(2)	(3)	(4)	(5)
26. Firmamızda, güvenlik politikalarımızı (süreçlerimizi) ihlal eden çalışanlar için resmi bir disiplin süreci vardır.	(1)	(2)	(3)	(4)	(5)
27. Firmadaki bilgisayarıma Mp3, video benzeri dosyalar indirebilirim.	(1)	(2)	(3)	(4)	(5)
28. Firmamız, önemli bilgiler paylaştığımızda karşıdan yazılı onay almamızı ister.(Rapor, Cari mutabakat vs.)	(1)	(2)	(3)	(4)	(5)

EK-2 (devam). Bilgi Güvenliği Farkındalığı Ölçeği

29. Yazılı onayların, ileride doğabilecek hukuksal problemleri engelleyeceğinin farkındayım.	(1)	(2)	(3)	(4)	(5)
30. Firmamızda, Dijital imzaya önem gösterilir.	(1)	(2)	(3)	(4)	(5)
31. Firmamız, önemli bir evrak silindiği zaman, işlemi yapan kullanıcıyı kayıtlardan <u>bulamaz</u> .	(1)	(2)	(3)	(4)	(5)
32. Firmamız, müşterilerimizin rızası olmadan onların bilgilerini başkalarıyla paylaşmaz .	(1)	(2)	(3)	(4)	(5)
33. Firmamızda, müşterilerimizin rızası olmadan onların bilgilerini başka amaçlarla kullanmaz.	(1)	(2)	(3)	(4)	(5)
34. Firmamız, müşterilerimizin bilgilerini başka kurumlarla paylaşmadan önce ilgili kişiye bilgi verir.	(1)	(2)	(3)	(4)	(5)
35. Firmamız, müşterilerimizin kişisel bilgilerini olası tehditlere karşı korur.	(1)	(2)	(3)	(4)	(5)
36. Kişisel bilgi mahremiyetin ne olduğunu biliyorum.	(1)	(2)	(3)	(4)	(5)
37. Müşterimle olan ilişkilerimde kişisel bilgi mahremiyete göre hareket ederim.	(1)	(2)	(3)	(4)	(5)

EK-3. Bilgi güvenliği farkındalığı ölçeği kullanım izin belgesi

<i>SİLOPİ MESLEK YÜKSEKOKULU</i>	
TARİH: 18 / 01 / 2021	
GAZİ ÜNİVERSİTESİ	
BİLİMSEL ARAŞTIRMA ve YAYIN ETİĞİ KURULLARI BAŞKANLIĞINA	
Kurulunuzdan onay alınması halinde Danışmanlığını Doç. Dr. Şahin Gökçearslan'ın yaptığı ve Sena NEZGİTLİ tarafından gerçekleştirilecek olan "Kamu Kurumu ve Özel Sektöre Yönelik Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme" başlıklı projede/araştırmada, tarafımdan geliştirilmiş/uyarlanmış olan Siber Riskler Karşısında Kobi'lerin Bilgi Güvenliği Farkındalıklarını Ölçen Bir Ölçek Geliştirme: Gaziantep Örnekleme Ölçeği'nin kullanılmasına izin veriyorum.	
ÖLÇEK SAHİBİNİN; UNVANI: Doktor Öğretim Üyesi ADI SOYADI: Cüneyt Çatuk	
+	
İŞ ADRESİ: Dicle mah. 23.cad.no:3 Silopi/Şırnak TELEFON: / E-POSTA: /	

EK-4. Etik Kurul Kararı

Çvrak Tarih ve Sayısı: 22.02.2021-E.32674



**T.C.
GAZİ ÜNİVERSİTESİ
Etik Komisyonu**

Sayı : E-77082166-302.08.01-32674
Konu : Bilimsel ve Eğitim Amaçlı

BİLİŞİM ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 26.01.2021 tarihli ve 73247369-302.08.01- 15065 sayılı yazı.

İlgi yazınız ile göndermiş olduğunuz, Enstitünüz Adli Bilişim Anabilim Dalı Yüksek Lisans Öğrencisi **Sena NEZGİTLİ'nin,** Doç.Dr.Şahin GÖKÇEARSLAN'ın danışmanlığında yürüttüğü "*Kamu Kurumu ve Özel Sektöre Yönelik Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme*" adlı tez çalışması ile ilgili konu Komisyonumuzun 16.02.2021 tarih ve 03 sayılı toplantısında görüşülmüş olup,

İlgilinin çalışmasının, yapılması planlanan yerlerden izin alınması koşuluyla yapılmasında etik açıdan bir sakınca bulunmadığına oybirliği ile karar verilmiş ve karara ilişkin imza listesi ekte gönderilmiştir.

Bilgilerinizi ve gereğini rica ederim.

Araştırma Kod No: 2021 - 179

Prof. Dr. İsmail KARAKAYA
Komisyon Başkanı

Ek:1 Liste

Bilgi Dağıtımına Kodu :BEA6A2VAY

Bu belge, güvenli elektronik imza ile imzalanmıştır.
Belge Tutarlı Adresi : <https://belgedogrulama.gazi.edu.tr/belgedogrulama.aspx>
--- 2 ---

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : NEZGİTLİ, Sena

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek Lisans	Gazi Üniversitesi / Adli Bilişim	Devam ediyor
Lisans	Gazi Üniversitesi / Elektrik-Elektronik Müh.	2014
Lise	Alparslan Anadolu Lisesi	2010

İş Deneyimi

Yıl	Yer	Görev
2018-Halen	Kamu Kurumu	Uzman
2016-2017	Merkez Anadolu Mühendislik	Proje Yöneticisi

Yabancı Dil

İngilizce

Yayınlar

- Nezgıtlı, S. ve Benzer, R. (2020). Avrupa Birlięi Siber Güvenlik Kanunu. *Journal of Information Systems and Management Research*, 2(1), 10-17.
- Gökçearslan, Ş., Nezgıtlı, S. ve Çakır, H. (2020). Bilişim suçu haberlerinin basında sunumu: 2009-2019 yılları arası çevrimiçi gazete haberleri örneklemleri. *Bilgi ve İletişim Teknolojileri Dergisi*, 2(2), 149-160.
- Nezgıtlı, S. (2021), *İngiltere ve Türkiye'nin siber güvenlik politikalarının karşılaştırılması*. Uzmanlık Tezi, Radyo ve Televizyon Üst Kurulu Strateji Geliştirme Dairesi Başkanlığı, Ankara. (Uzmanlık tezinden üretilmiştir)



GAZİLİ OLMAK AYRICALIKTIR..