Atıf/ Citation: Nezgitli, S. & GökçeArslan, Ş. (2022). Kamu kurumu ve özel sektöre yönelik bilgi güvenliği farkindaliği üzerine bir inceleme. *Instructional Technology and Lifelong Learning, 3* (1), 19-44. DOI: 10.52911/itall.1115701

Instructional Technology and Lifelong Learning Vol. 3, Issue 1, 19-44 (2022)

https://dergipark.org.tr/tr/pub/itall

ITALL

Research Article

ISSN: 2717-8307

Review on Information Security Awareness for Public Institutions and Private Sectors

Sena NEZGİTLİ *[1], Şahin GÖKÇEARSLAN [2]

ARTICLE INFO

Article history:
Received: 30/04/2022
Accepted: 25/05/2022
Online: 30/06/2022
Published: 30/06/2022

Keywords:
Information security
Information security awareness
Corporate information security
Information security culture

ABSTRACT

The aim of this study is to measure the information security awareness levels of people working in public institutions and private sectors. The research, using the screening model, was carried out with the participation of 138 people working in the field of informatics in various public institutions and private sectors in Ankara. According to the results of the study in which this model was used, there was no significant difference in terms of gender, institution type, age, position, the source from which the concept of information security was learned, and the frequency of training/course on information security awareness. A significant difference was observed in terms of providing training/course on information security awareness in the workplace and having an information security policy of the workplace, the degree of benefit of the information security awareness training/courses given at the workplace and the degree of implementation of the information security policy. The research results are discussed in the context of information security culture.

Kamu Kurumu ve Özel Sektöre Yönelik Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme

MAKALE BİLGİ

Makale Geçmişi:
Geliş: 30/04/2022
Kabul: 25/05/2022
Çevrimiçi: 30/06/2022
Yayın: 30/06/2022

Anahtar Kelimeler:
Bilgi güvenliği
Bilgi güvenliği farkındalığı
Kurumsal bilgi güvenliği
Bilgi güvenliği kültürü

ÖZET

Bu çalışmanın amacı, kamu kurumu ve özel sektörde çalışan kişilerin bilgi güvenliği farkındalık düzeylerini ölçmektir. Tarama modeli kullanılan araştırma, Ankara ilinde çeşitli kamu kurumu ve özel sektörde bilişim alanında çalışan 138 kişinin katılımı ile gerçekleşmiştir. Araştırma sonuçlarına göre cinsiyet, kurum türü, yaş, pozisyon, bilgi güvenliği kavramının öğrenildiği kaynak, bilgi güvenliği farkındalığı hakkında eğitim/kurs verilme sıklığı bakımından anlamlı farklılaşma olmamıştır. İşyerinde bilgi güvenliği farkındalığı hakkında eğitim/kurs verilme ve işyerinin bilgi güvenliği politikasına sahip olma, işyerinde verilen bilgi güvenliği farkındalığı eğitim/kursların fayda derecesi ve bilgi güvenliği politikasının uygulanma derecesi bakımından anlamlı fark gözlenmiştir. Araştırma sonuçları bilgi güvenliği kültürü bağlamında tartışılmıştır.

* *Corresponding Author, snnzgtli@gmail.com*
[1]*snnzgtli@gmail.com, Gazi University, Digital Forensics, Ankara, Turkey*
[2]*sahingokce@gmail.com, Gazi University, Distance Education Center, Ankara, Turkey*

Extended Summary

Problem Statement

The transfer of information assets to cyber space has brought disadvantages as well as advantages. The increasing number of people and devices in cyberspace has started to pose a threat to the existence of information (Ermiş, 2018) and methods to ensure information security have been developed in the face of this threat. In order to keep information safe, information security awareness studies have started to be carried out for human, who is the weakest link in security, as well as eliminating technological vulnerabilities. As a result of these studies, it was aimed to raise awareness of the human factor by creating a culture of information security awareness (Chan & Mubarek, 2012). Institutional structuring is required to achieve this goal (El-Haddadeh, Tsohou, & Karyda, 2012). Awareness activities carried out thanks to the institutional structuring are progressing in a more disciplined manner. For information security awareness, first of all, awareness levels of employees should be measured and awareness-raising activities should be handled in line with the results. A prototype was developed by Kruger and Kearney (2006), a scale was developed by Erdoğdu, Gökoğlu and Kara (2020), a questionnaire was developed by Velki, Solic and Ocevcic (2014), and there are other methods developed on the subject. These developed methods have been included in many studies.In this study, the "information security awareness scale" study was used to measure the information security awareness levels for the determined public institutions and private sector employees and the results were examined. In this study, the "information security awareness scale" study was used to measure the information security awareness levels for the determined public institutions and private sector employees and the results were examined.

Method

In this study, screening model was used as a qualitative research method. 138 people working in various public institutions and private sectors participated in the information security awareness scale study. 33 of the participants were women and 105 were men. The scale used consists of 37 questions and 4 sub-dimensions in 5-point Likert type prepared by Çatuk (2018). Data analysis was done in SPSS 25.0 program. Since the data did not show normal distribution, Mann Whitney U and Kruskal Wallis H tests were used. As a result of the analysis, Cronbach's Alpha internal consistency coefficient (α) was found to be .96. If this coefficient is higher than 0.81, it is stated that the scale has high reliability (Özdamar, 2002). Therefore, this study is seen to be of high reliability.

Findings

In this study, the gender factor did not make a statistically significant difference on information security awareness, as in the study of Karabatak and Karabatak (2019), Quisumbing (2019). The age factor of the employees did not make a statistically significant difference on the awareness of information security, just like in the study of Çelikçöp and Yarar (2019). In the study, the type of institution does not make a statistically significant difference on information security awareness. Just like Ceylan (2019)'s study, the educational status of the employees did not make a statistically significant difference on the awareness of information security. The positions of the employees in the company did not make a statistically significant difference on the awareness of information security, just as in the study of Değer (2020). In addition, as a result of the study, it was observed that the type of source from which the participants learned the concept of information security did not make a statistically significant difference on information security awareness.

Factors affecting information security awareness in the study; The company has an information security policy, the degree of implementation of this policy, training/course on information security awareness in the company, and the degree of benefit of the training/course provided. These four elements made a statistically significant difference for information security awareness. In addition, according to the results, the frequency of training/course on information security awareness in the company did not make a statistically significant difference. In the study of Yayla (2018), it was argued that information security awareness trainings would contribute positively to information security awareness, while in the study of Yıldız and Atasoy (2016), it was argued that having an information security policy in the company would contribute to raising the level of information security awareness of employees. In these two studies, it was stated that the awareness of information security depends on the company's having an effective information security policy and quality application activities that will increase the level of information security awareness by making similar conclusions and inferences with this study.

Discussion and Conclusion

When the research results and the results of the previous studies are examined, the awareness of information security depends on the fact that the company has an effective information security policy and that this policy is adopted and implemented by the employees of the institution, rather than the demographic characteristics of the people. Of course, one of the factors on which information security awareness depends is to raise awareness of company employees about information security awareness, regardless of gender, age, education status and

position variables, and that these awareness-raising activities have a rich content. In short, providing information security awareness depends on an effective information security policy and correct awareness-raising activities for individuals.

1. Giriş

İnsanlık, varoluşundan beri çevresini ve dünyasını anlama gayreti ile bilgi edinmek istemiştir (Toprak, 2020, s. 322). Bilgi, insanlık tarihinin kökeni kadar eski bir olgu olarak karşımıza çıkmaktadır (Ağır ve Turhan, 2014, s. 285). Bilginin varoluşu ile başlayan bilgi edinme serüveni, insanların diğer insanlarla iletişime geçmesi ile artmış ve edinilen bu bilgiler insanlık tarafından kullanılmaya başlanmıştır. İnsanlığın iletişim kurmasında bilgi ve bilgi edinme yolları, yazının icadına kadar sözel biçimde yapılmıştır. Edinilen bilgi birikiminin artmasıyla bu bilgiler sözel biçimden yazı aracılığıyla farklı materyallere aktarılmaya başlanmıştır. Bu durum, bilginin hem kalıcı olarak iletilmesini hem de bilginin değişimini hızlandırmıştır (Atılgan, 2006, s. 1). Bilginin iletimi ve değişimi, sadece bilginin yazıya aktarılmasıyla sınırlı kalmamıştır. Yazının yanı sıra bilgi ve iletişim teknolojilerinin gelişmesiyle birlikte bilgi elektronik ortama aktarılmıştır. Bu durum bilginin iletimine ve değişim serüvenine yeni bir soluk getirmiştir. Bilginin elektronik ortama aktarılması; bilgisayarlarla daha fazla gelişmiş ve internet olanaklarıyla (Dilek, 2016, s. 88) ivme kazanarak devam etmiştir. Bu ivme internetin yaygınlaşmasıyla beraber bölgesel bağlamdan edinilen ve paylaşılan bilgiye küresel bir boyut kazandırmıştır (Korhan, 2017, s. 76). Bu küresel boyut sayesinde bilgi edinme ve paylaşma olgusu zaman ve mekândan bağımsız olarak her an gerçekleşme imkânı bulmuştur.

Bilgi varlığındaki gelişmeler ve değişimler, sanal ortam ifadesini de değiştirerek; 1982 yılında William Gibson tarafından kullanılan siber uzay kelimesi ile anılmaya başlanmıştır (Fourkas, 2004, s. 1). Siber uzay sayesinde bilgi, zaman ve mekândan bağımsız olarak iletilme ve değiştirilme imkânı bulmuştur. Ancak zaman içerisinde teknolojinin ilerlemesi, internet kapasitesinin gelişmesi, siber uzayda var olan insan ve bilgisayarın yanı sıra başka cihazların da bu ortama dâhil olmasına yol açmıştır. Bu sayede bilgi, sadece bilgisayarlarda üretilen ve bilgisayarlar arasında paylaşılarak değiştirilen bir olgu olarak kalmamıştır. Siber uzayda bilgi, *Nesnelerin İnterneti* (Internet of Things-IoT) olarak adlandırılan (Keertikumar ve diğerleri, 2015, s. 805) ve internete bağlanabilen tüm akıllı cihazlar ile de paylaşılabilmiştir. Nesnelerin İnterneti veri zenginliğini sağlamakla birlikte, bilgi dünyasında da değişimin öncüsü konumundadır (Gökçearslan ve Sarıtepeci, 2021, s. 352). CISCO, *Yıllık İnternet Raporunda* 2023 yılında internete bağlı olan cihaz sayısının 29 milyardan fazla olacağı biçiminde öngörüde bulunmuştur (Cisco, 2020, s. 13). Güncel başka bir raporda ise, 2030 yılına kadar Nesnelerin İnternetine bağlı olan cihaz

sayısının 125 milyara çıkacağı belirtilmiştir (IHS Markit, 2017, s. 2). Geleceğe yönelik öngörülen cihaz sayısındaki bu artış ile siber uzay kontrolsüzce büyüyerek bilgi varlığını tehdit edebilir. Bu durum, bilgi varlığına hızlı erişim ve depolama imkânı sunsa bile siber uzayda artan kişi ve cihaz sayısı bilgi varlığına çeşitli tehditler oluşturarak güvenliğine zarar vermeye başlayan olumsuz faaliyetleri ortaya çıkarmıştır (Gökçearslan ve diğerleri, 2020, s. 156). Bu tehdit, kötü niyetli kullanıcılara daha fazla araçla yetkisiz erişim imkânı sağlayarak bilgi güvenliğini riske atmaktır. Kötü niyetli ve yetkisiz kullanıcıların bilgi güvenliğini riske atması, bilgi için hızlı erişim ve paylaşımın öneminden ziyade bilgi güvenliğinin nasıl sağlanacağı konusunu gündeme getirmiştir. Siber uzayda bilgi güvenliğinin sekteye uğramaması için iyi bir savunma teknolojisine ve farkındalık düzeyi yüksek olması beklenen insan faktörüne odaklanılması gerekmektedir (Henkoğlu ve diğerleri, 2012, s. 394).

Her ne kadar güçlü savunma teknolojisi ile sistem açıkları kapatılabilse de sistemle teması bulunan kişilerin konu hakkında bilinçli olmaması bilgi güvenliğini ciddi olarak tehlikeye atmaktadır. Siber uzayda bilgi güvenliğini tehdit eden saldıranların çoğunluğu, güvenlik halkasında zayıf zincir olarak görülen insana (Barrett, 2003, s. 57) yönelik gerçekleştirilmektedir. Bilgi güvenliğinin sağlanması için bireylerin farkındalık düzeyinin arttırılması gereklidir (Shropshire ve diğerleri, 2015, s. 186). Bu nedenle, bilgi güvenliğinin sağlanmasında bilgiye erişen bireylerin bilgi güvenliği farkındalığı hakkında bilinçlendirilmesi oldukça önemlidir.

Bilgi güvenliği farkındalığı sadece bireyler için değil kurumlar açısından da önemlidir. Ponemon Institute tarafından yapılan, 2017 yılının sonunda 612 yöneticinin (bilgi güvenliği sorumlu başkanlar ve bilgi sistemleri grup başkanlarından oluşan) katılım gösterdiği araştırmada, şirketler için en büyük güvenlik tehdidinin insan faktörü olduğu belirtilmiştir (Ponemon Institue, 2018, s. 2). Ayrıca uluslararası bir kuruluşun *Siber İstihbarat Bölümü* raporuna göre şirketlere yönelik e-posta dolandırıcılığının yıllık ortalama 26 milyar dolar hacme sahip olduğu belirtilmiştir (Agari, 2020, s. 4). Bu araştırmalarda görüldüğü üzere çalışanların bilerek veya bilmeyerek oluşturacakları güvenlik zafiyetinin kurum için maddi ve itibar yönünden kayba neden olabileceği belirtilmektedir (Yeniman Yıldırım, 2018, s. 2). Bu nedenle işyerlerinde bilgi güvenliği farkındalığı ve kültürü oluşturulması önemli görülmektedir. Bu oluşum kurumsal içerik yönetimi organizasyonu içinde gereklidir (Çakmak ve Külcü, 2011, s. 268). Kurumsal bilgi güvenliği farkındalığı ve kültürünün oluşturulmasındaki ilk adım, çeşitli yöntemlerle (anket, görüşme vb.) çalışanlara yönelik bilgi güvenliği farkındalık düzeyinin belirlenmesi olabilir. Bu durumu, belirlenen düzey doğrultusunda işyeri için ihtiyaçlara göre bir yol haritasının oluşturulması takip edebilir. Bu iki adım işyeri ve çalışanlar için bilgi güvenliği farkındalığı konusunda önem arz etmektedir.

2. Literatür Taraması

2.1. Bilgi Güvenliği Kavramı ve Unsurları

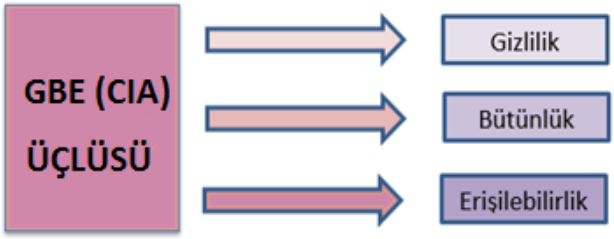
Bilgi güvenliği doğası gereği birçok kavram ve unsuru içinde barındırmaktadır. Bu nedenle öncelikle bilgi güvenliğinin oluşmasını sağlayan bilgi kavramının tanımına bakmak anlamlı olacaktır. Bilgi kavramı, gözlem ve araştırma ile öğrenilen gerçek olarak ifade edilebilir (Yenal, 2009, s. 126). Siber uzayda ise bilgi kavramı, işlenmemiş parçaların yani verilerin işlenmesi ile anlam kazanarak bir değere sahip olma durumudur (Özdemir ve Uluyol, 2021, s. 651). Bilgi kavramının tanımından yola çıkarak bilgi güvenliği, işlenmiş verinin yetki dâhilinde kaynaktan alıcıya gidene kadar gizli bir biçimde, değişikliğe uğramadan ve bütünlüğünün muhafaza edilerek iletilmesini ifade eder (Pfleeger, 1997, s. 15). Bilgi güvenliği, bilgiye izni olmayan ve yetki erişimi verilmemiş kişi ve sistemler tarafından bilgiyi ifşa etme, değiştirme, bozma, yok etme gibi olumsuz faaliyetlere karşı bilgiyi koruma çabasıdır (Şen ve Yerlikaya, 2013, s. 677). Kısacası bilgi güvenliği, bilgiyi siber uzayda tehdit eden tüm unsurlara karşı koruma mücadelesidir.

Siber uzayın kapasitesi ve faaliyet alanı düşünüldüğünde bilgi güvenliğine yönelik birçok tehdit unsuru mevcuttur. Bu unsurlar; kimi zaman teknolojik ilerlemeler sonucunda kaynaklanan problemler (kötücül yazılımlar) (Derin ve Gençoğlu, 2020, s. 165) olarak karşımıza çıkarken kimi zamanda bilginin varlığını sürdürdüğü sistem veya sistemlere yetkisiz erişim sağlayan insan faktörü (Demir, 2005, s. 148) olarak karşımıza çıkmaktadır. Bilginin varlığını siber uzayda tehdit eden bu unsurlara karşı, bilgi güvenliği unsurlarının geliştirilmesi, bilgi güvenliği kültürü ve güvenliğin en zayıf halkası olan insanın bilinçlendirilmesi önemlidir (Hai-Jew, 2019, s. 206; Lineberry, 2007, s. 44).

Bilgi güvenliğini sağlamanın ilk adımı, güvenlik için hangi unsurlara ihtiyaç duyulacağının belirlenmesidir. Bilgi güvenliğini sağlayan temel unsurlar bilginin güvende kalması adına olması gereken unsurlardır. Bu unsurlar, bilginin gizliliğinin sağlanması, bilgiye erişilebilirlik ve bilginin bütünlüğünün muhafaza edilmesi gibi temel amaçlar taşır. Bilgi güvenliği adına erişilebilirlik, gizlilik ve bütünlük unsurları, McCumber (1991) tarafından geliştirilen bilgi güvenliği modelinde ilk olarak yer almıştır. Bu unsurlar, GBE (CIA) üçlüsü (Sumathi ve Sundaram 2015, s. 1; Von Solms ve Van Niekerk, 2013, s. 98) olarak da adlandırılmaktadır.

Şekil 1.

GBE (CIA) Üçlüsü (Sumathi ve Sundaram 2015, s. 1; Von Solms ve Van Niekerk, 2013, s.98)



Zaman içerisinde bu model ve temel unsurlara ek olarak bilgi güvenliği için yeni modeller ve yeni unsurlar eklenmiştir. Ahlfeldt ve diğerleri (2007) tarafından geliştirilen modelde; gizlilik, bütünlük, erişilebilirlik unsurlarının yanı sıra hesap verilebilirlik unsurunu da yer almıştır ve Röhrig (2003) de bu dört unsurun güvenlik modelinde mevcut olmasını gerektiğini savunmuştur. Cherdantseva ve Hilton (2013) geliştirdiği bilgi güvenliği modelinde; sadece gizlilik, bütünlük ve erişilebilirlik unsurlarını kullanmakla kalmamış ayrıca güvenilirlik, hesap verilebilirlik, denetlenebilirlik, inkâr edememe ve mahremiyet unsurlarına da yer verilmiştir. Bu unsurlar sayesinde, bilgiyi güvende tutarak onu koruyacak farklı bilgi güvenliği modelleri oluşturulmuştur (Boyacı ve diğerleri, 2016, s. 32). Temel unsurlardan gizlilik, bilgiye erişimi sadece yetkili kişi ve sistemlere verirken (Abbas ve diğerleri, 2015, s. 2393); bütünlük, bilginin doğru ve eksiksiz bir biçimde korunmasını sağlarken (Whitman ve Mattord, 2021, s. 202); erişilebilirlik ise, bilgi ve bilgi kaynaklarının izne sahip yetkili kişilerce kullanılmasını (Tryfonas ve diğerleri, 2000, s. 38) sağlamaktadır. Diğer unsurlardan güvenilirlik, bilginin içinde bulunduğu sistemin belirli koşullar ve süreç içerisinde bilgiye erişim sağlama imkânını (Jonsson, 2006, s. 2); mahremiyet, bilgi ve bilgi varlığının gizliliğinin korunması adına yürütülen faaliyetleri (Nissenbaum, 2004, s. 123); hesap verilebilirlik, sisteme yetki erişimi olan kişilerin sistemde yaptıkları işlemler için sorumluluk alarak gerekli görüldüğünde yaptıkları işlemleri açıklama yükümlülüğünü (Çalıkuşu ve diğerleri, s.4); inkâr edememe, sistemde yetkili kullanıcının yaptığı işlemleri reddetmesi durumunda işlemleri kendisinin yaptığına dair kanıt sunulmasını (Canbek ve Sağıroğlu, 2006, s. 170); denetlenebilirlik ise, sistemde yapılan faaliyetlerin izlenebilmesini ifade etmektedir (Konacaklı, 2019, s. 24). Bilgi güvenliğinin sağlanması adına bu unsurlar büyük önem taşımaktadır.

Bilgi güvenliğini sağlamanın ikinci adımı, bilgi güvenliği kültürünün oluşturulmasıdır. Bilgi güvenliği kültüründen söz edebilmek için kurumsal bir yapılanma veya örgütsel bir oluşumdan (Baran ve Şener, 2020, s. 411) bahsedilmesi gerekir. Bu nedenle etkili bir bilgi güvenliği kültürü; kurumsal bilgi güvenliği politikası, kurumsal bilgi güvenliği yönetimi ve oluşturulan uluslararası standartlar ile mümkündür. Kurumsal bilgi

güvenliği politikası, kuruluş içindeki bilgi varlığının korunması adına yapılacakların belirlendiği bir dizi faaliyetleri içeren bir rehberdir (Mears ve Von Solms, 2004, s. 6). Bu rehber, bilgi güvenliğinin sağlanması ve yapılacakların belirlenmesi için önemlidir.

Bilgi güvenliğini sağlamanın üçüncü adımı, güvenliğin en zayıf halkası olarak görülen insan (Colwill, 2009, s. 2) için yapılacak bilinçlendirme faaliyetleridir. Bu adım, bilgi güvenliği farkındalığı kavramını oluşturarak kurumlar için bilgi güvenliği farkındalığının sağlanma yöntemlerini gündeme getirmiştir.

2.2. Kurumsal Bilgi Güvenliği Farkındalığı ve Kültürü

Kurumsal bilgi güvenliği farkındalığının temelini, siber uzayda verilen yetki dâhilinde bilgi varlığına ulaşma, bilgi varlığını değiştirme ya da iletme yetkisi bulunan kuruluş bünyesindeki çalışan insanlara yönelik oluşturulan çeşitli faaliyetler oluşturmaktadır. Bu faaliyetler; çeşitli kursları (Kritzinger ve Von Solms, 2010, s. 2), programları (Van Niekerk, 2005, s. 2) ve eğitimleri (Wilder, 2019, s. 4) kapsayarak insanların bilinçsiz davranışlarından ötürü kaynaklanabilecek tehdit unsurları konusunda kuruluş içinde denetim mekanizması (Choi ve Han, 2015, 476) oluşturur. Tüm bu faaliyetler kurumsal bilgi güvenliği farkındalığı kültürünün oluşmasına (Box ve Pottas, 2013, s. 1095) yardımcı olur ve bilgi güvenliği faaliyetleri ile risk yönetimine de katkı sağlar (Ateş ve Güneş, 2016, s. 41) Sağlanacak eğitim, kurs ve programlar kuruluşun ve çalışanların ihtiyaçları doğrultusunda hazırlanmalı ve bu programların sürekliliği sağlanmalıdır (Desman, 2001, s. 9). Unutulmaması gereken en önemli durum bilgi ve bilgi güvenliği varlığına yönelik kuruluşların sürekli bir risk altında bulunduğudur. Kısacası, kurumsal bilgi güvenliği farkındalığının temelini oluşturan insan faktörüne sürekli bir iyileştirme yapılmalıdır. Yapılan bu iyileştirmelerin insanlar üzerinde etkisini ölçmek için çeşitli yöntemlerle (anket, ölçek vb.) çalışanlardan dönüt alınmalıdır. Alanyazında belirli meslek gruplarına ve belirli sektörde çalışan kişilere yönelik çalışmalar mevcut olsa bile iki farklı sektör çalışanlarının bilgi güvenliği farkındalığını ölçümlemek üzerine bir çalışmaya alanyazında rastlanmamıştır. Bu çalışmadaki temel amaç, kamu kurumu ve özel sektörde çalışan bireylerin bilgi güvenliği farkındalık düzeylerini karşılaştırmak olacaktır. Ayrıca bilgi güvenliği farkındalığının; cinsiyet, yaş, kurum türü, öğrenim durumu, çalışılan pozisyon, bilgi güvenliği kavramının öğrenildiği kaynak, 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 değişkenleri bağlamında analiz edilmesidir.

2.3. Araştırmanın Amacı

Araştırmanın amacı; kamu kurumu ve özel sektörde çalışan bireylerin bilgi güvenliği farkındalık düzeylerinin

çalıştıkları kurum türüne göre değişiklik gösterip göstermediğini ölçerek iki sektör arasında kıyaslama yapmaktır. Araştırmanın problemi; Ponemon Institue (2018) ve Agari'nin (2020) iş yerleri için çalışan kişilerin bilgi güvenliği farkındalık düzeylerinin önemini vurgulamaktadır. Ayrıca Özkaya ve Şengül'ün (2006) çalışmasında kamu kurumunda çalışanlar ile özel sektörde çalışanlar arasında iş etiği konusunda farklı davranışlar olduğu belirtilmiştir. Bu doğrultuda iki sektör çalışanları arasında bilgi güvenliği farkındalığı konusunda da farklı davranış gösterme eğiliminin olup olmadığı hakkında bir problem düşünülmüştür.

Araştırmanın soruları; bu amaç doğrultusunda aşağıdaki sorulara cevap aranmıştır:

1. Katılımcıların kurum türüne göre bilgi güvenliği farkındalık düzeyleri arasında anlamlı bir fark var mıdır?
2. Katılımcıların bilgi güvenliği farkındalığı; cinsiyet, yaş, öğrenim durumu, iş yerindeki çalışma pozisyonu, bilgi güvenliği kavramını öğrendiği kaynak, iş yerinde bilgi güvenliği hakkında kurs verilme durumu, kurs verilme sıklığı, kursun fayda derecesi ve kurumun bilgi güvenliği politikası ile bu politikanın uygulanma derecesine göre anlamlı bir fark oluşturmakta mıdır?

3. Yöntem

3.1. Araştırmanın Deseni

Kamu kurumu ve özel sektörden oluşturulan çalışma grubu için bilgi güvenliği farkındalık düzeyini ölçmek için tarama modeli kullanılmıştır. Tarama modeli, içinde bulunulan durumu betimleyen ve nesneleri kendi içerisinde olduğu gibi tanımlayan bir modeldir (Karasar, 2008, s. 77).

3.2. Çalışma Grubu

Araştırmanın çalışma grubu, 2021 yılında Ankara ilinde bilişim alanında kamu kurumu ve özel sektörde çalışan 138 kişiden oluşmaktadır. Kurumlarda bilgi güvenliği uygulamalarını bilgi işlem dairesi çalışanları sürdürmektedir (Öztemiz ve Yılmaz, 2013, s. 95). Bu nedenle katılımcılar kamu ve özel sektörlerde çalışan bilgi işlem personelinden Basit Rastgele Örnekleme yöntemi kullanılarak seçilmiştir. Basit rastgele örnekleme yöntemi, araştırma grubu için örneklem seçiminde tercih edilen en temel yöntemlerden biridir (Karakülah, 2006, 1). Çalışma grubuna ait demografik özelliklere Tablo 1'de yer verilmiştir.

Tablo 1

Araştırmadaki Katılımcıların Demografik Özellikleri

Değişken	Grup	f	%
Cinsiyet	Kadın	33	23,9
	Erkek	105	76,1
Kurum Türü	Kamu kurumu	85	61,6
	Özel sektör	53	38,4
Yaş	20-29 yaş arası	50	36,2
	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
	Ön Lisans	11	8,0
	Lisans	75	54,3
	Yüksek Lisans	46	33,4
	Doktora	5	3,6
Pozisyon	Yönetici	22	15,9
	Teknik personel	81	58,7
	İdari personel	35	25,4
Bilgi güvenliği kavramını hangi kaynaktan öğrendiniz?	Akademik kaynak	38	27,5
	Alınan eğitim	85	61,6
	Medya	12	8,7
	Çevredeki kişiler	3	2,2
İşyerinizde bilgi güvenliği politikası mevcut mu?	Evet	132	95,7
	Hayır	6	4,3
İşyerinizde bilgi güvenliği politikasının uygulanma derecesi nedir?	Oldukça uygulanıyor	69	50
	Uygulanıyor	52	37,7
	Karasızım	12	8,7
	Uygulanmıyor	4	2,9
	Hiç uygulanmıyor	1	0,7
Bilgi güvenliği farkındalığı hakkında eğitim/kurs veriliyor mu?	Evet	121	87,7
	Hayır	17	12,3
**Bilgi güvenliği farkındalığı üzerine ne sıklıkla eğitim/kurs veriliyor?	Üç ayda bir	20	16,5
	Altı ayda bir	58	47,9
	Yılda bir	28	23,2
	Bir yıldan fazla	15	12,4
**Bilgi güvenliği farkındalığı eğitimleri/kursları ne kadar faydalı?	Çok faydalı	41	33,9
	Faydalı	65	53,7
	Karasızım	10	8,3
	Faydasız	5	4,1

Not. ** "Bilgi güvenliği farkındalığı hakkında eğitim/kurs veriliyor mu?" sorusuna evet cevabı veren katılımcıları yansıtmaktadır.

Tablo 1 incelendiğinde araştırmadaki çalışma grubu içinde bulunan katılımcıların, %23,9'u (33) kadın ve %76,1'i (105) ise erkeklerden oluşmaktadır. Çalışma grubundaki katılımcıların %61,6'sı (85) kamu kurumunda çalışırken %38,4'ü (53) ise özel sektörde çalışmaktadır. Çalışma grubunda, ilk sırayı %43,5 (60) ile 30-39 yaş, ikinci sırayı %36,2 (50) ile 20-29 yaş ve üçüncü sırayı da %16,7 (23) ile 40-49 yaş aralığındaki bireyler almaktadır. Çalışma grubunda, ilk sırayı %54,3 (75) ile lisans, ikinci sırayı %33,4 (46) ile yüksek lisans ve üçüncü sırayı %8 (11) ile ön lisans mezunu bireyler almaktadır. Çalışma grubunda ilk sırayı %58,7 (81) ile teknik personel**,** ikinci sırayı %25,4 (35) ile idari personel ve üçüncü sırayı %15,9 (22) ile yönetici kadrosunda çalışan bireyler almaktadır. Çalışma grubunda bilgi güvenliğinin öğrenildiği kaynak bakımından; ilk sırayı %61,6 (85) ile alınan eğitim, ikinci sırayı %27,5 (38) ile akademik kaynak ve üçüncü sırayı da %8,7 (12) ile medya almaktadır. Çalışma grubundaki katılımcıların bilgi güvenliği farkındalığı hakkında işyerinde eğitim/kurs verilme durumuna %87,7'si (121) evet derken %12,3'ü (17) hayır yanıtını vermiştir. Çalışma grubunda işyerinde eğitim/kurs alan personelin eğitim/kurs alma sıklık derecesine göre; ilk sırada %47,9 (58) ile altı ayda bir, ikinci sırada %23,2 (28) ile yılda bir ve üçüncü sırada %16,5 (20) ile üç ayda bir seçeneği almaktadır. Eğitimi alan personelin kursu faydalı bulma derecesinde ilk sırayı %53,7 (65) ile faydalı, ikinci sırayı %33,9 (41) ile çok faydalı ve üçüncü sırayı %8,3 (10) ile kararsızım seçeneği almaktadır. Çalışma grubundaki katılımcılar, işyerinde bilgi güvenliği politikasının mevcut olma durumu hakkında; %95,7'i (132) evet yanıtını verirken %4,3'ü (6) ise hayır cevabı vermiştir. Çalışma grubunda, işyerinde bilgi güvenliği politikasının uygulanma derecesine göre; ilk sırayı %50 (69) ile oldukça uygulanıyor, ikinci sırayı %37,7 (52) ile uygulanıyor ve üçüncü sırayı %8,7 (12) ile kararsızım seçeneği almaktadır.

3.3. Veri Toplama

Veri toplama aracında araştırmaya uygun olarak nicel veri toplama aracı olan ölçek kullanılmıştır. Bu ölçekte, demografik özelliklere yönelik on bir soru ve bilgi güvenliği farkındalığı kısmında ise otuz sekiz soru yer almaktadır. Ölçek, iki bölümden meydana gelmektedir.

Bilgi Güvenliği Farkındalığı Ölçeği

Bu çalışmada, Çatuk (2018)'un geliştirdiği *"Bilgi Güvenliği Farkındalığı Ölçeği"* kullanılmıştır. Bu ölçme aracı için açımlayıcı ve doğrulayıcı faktör analizi yapılmıştır. Ölçek, 5'li likert tipinde (1=Kesinlikle katılmıyorum, 2=Katılmıyorum, 3=Kararsızım, 4=Katılıyorum, 5=Kesinlikle katılıyorum) ve 33 maddeden meydana gelmiştir. Çatuk'un (2018) çalışmasında Cronbach's Alpha iç tutarlılık katsayısı (α) .954 olarak ölçülmüş ve ölçek, dört

faktörden meydana gelmektedir. Bu çalışmada ise Cronbach's Alpha iç tutarlılık katsayısı (α) .96 olarak ölçülmüştür. Ölçeğin güvenilirliği, Cronbach's Alpha katsayısının aldığı değere bağlı olup bu değer .70 ve.70'den büyükse ölçek güvenilirdir (Nunnally, 1975, s. 10). Buna göre ölçek %96 oranında güvenilirdir. Bu 4 faktör sırasıyla bilgi güvenliğinin de unsurları olan "Gizlilik", "Bütünlük", "Mahremiyet" ve "Erişilebilirliktir". Ölçek toplam varyansın %67,33'ünü açıklamaktadır. Bu oranı, %42,17'sini "Gizlilik", %10,16'sını "Bütünlük", %8,56'sını "Mahremiyet" ve %6,44'ünü "Erişilebilirlik" faktörü meydana getirmektedir (Çatuk, 2018, s. 88-89).

3.4. Veri Toplama Süreci

Veri toplamak için gerçekleştirilen ilk adım, Gazi Üniversitesi Etik Komisyonuna başvurularak gerekli izinlerin alınmasıdır. Etik Komisyonundan alınan izin doğrultusunda, veri toplama aracı işyerindeki insan kaynakları aracılığıyla katılımcıların kurumsal e-postalarına gönderilerek uygulanmıştır. Çalışmadaki sorulara yanıt vermeden önce kişilere çalışmaya gönüllülük esası ile katılacaklarını, kişisel bilgilerinin alınmayacağı, istenilirse çalışmadan ayrılabilecekleri ve toplanan verilerin sadece bilimsel amaç doğrultusunda kullanılacağı hakkında bilgilendirme sağlanmış ve kişilerden katılım onayı alınmıştır.

3.5. Veri Analizi

Çalışma sırasında toplanan veriler IBM SPSS 25 programında analiz edilmiştir. Analizlerde ölçüm puan ortalaması alınmış ve betimsel istatistik kullanılmıştır. Betimsel istatistik, nicel analizler için kullanılan klasik bir yöntemdir ve toplanan verilerin özetlenerek açıklanmasını sağlar (Suleymanova, 2015, s. 20).

Normalliğin Sınanması

Verilerin dağılımına ilişkin bilgi edinmek adına normalliğin sınanması, normallik testlerinin uygulanması ile öğrenilir (Ballı ve Önder, 2019, s. 519). Normalliğin sınanması, ölçüm ortalamasının çarpıklık-basıklık ve Kolmogrov-Smirnov testi ile gözden geçirilebilir (Varlı ve Uluçınar Sağır, 2019, s. 711).

Alanyazında normalliğin sınanması için çarpıklık ve basıklık değer aralıkları farklılık gösterebilmektedir. Verilerin normal dağılıma sahip olabilmesi için çarpıklık ve basıklık değerlerinin -3 ile +3 değer aralığında olması gerekir (Kalaycı, 2008, s. 209). Bu çalışmada, çarpıklık (-1,859) ve basıklık değeri (+3,475) olarak bulunmuştur. Bu değerlerin, alanyazında belirtilen çarpıklık ve basıklık değer aralığının dışında olduğu görülmektedir. Aynı zamanda bu çalışmada normalliğin sınanması için bakılacak diğer değer de Kolmogrov-Smirnov testinin sonucunda ortaya çıkan p değeridir. Bu çalışmada p değeri, 0,000 olarak bulunmuştur. P değeri 0.05'ten küçük olduğu için (Yoccoz, 1991, s. 107) veriler normal dağılmamaktadır. Veriler normal dağılım göstermediğinden

ikili küme karşılaştırmalarında Mann-Whitney U, ikiden fazla küme karşılaştırmalarında Kruskal-Wallis H istatistiksel testleri uygulanmıştır (Şimşek ve Altınkurt, 2009, 1; Demirel ve diğerleri, 2016, s. 10).

4. Bulgular

Bu bölümde analiz edilen verilerden çıkan sonuçlar neticesinde elde edilen bulgulara yer verilmiştir. Çalışmaya katılanların bilgi güvenliği farkındalığı ölçeğinden elde edilen toplam puanların cinsiyet, kurum türü, yaş, öğrenim durumu, pozisyon, bilgi güvenliği kavramının öğrenildiği kaynak, 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 sorulara verilen cevaplar doğrultusunda elde edilen sonuçlar belirtilmiştir. Verilerin normal dağılım göstermemesinden dolayı parametrik olmayan testler seçilmiştir. Mann Whitney U ve Kruskal Wallis H testleri uygulanmıştır.

Çalışmanın cinsiyete göre bilgi güvenliği farkındalığı ile ilgili Mann Whitney U testi sonucu Tablo 2'de verilmiştir.

Tablo 2

Cinsiyete Göre Bilgi Güvenliği Farkındalığı İle İlgili Mann Whitney U Testi Sonucu

Cinsiyet	n	Sıra ortalaması	Sıra toplamı	U	p	Anlamlı fark
Kadın	33	70,42	2324	1715,5	0,93	Yok
Erkek	105	69,21	7267			
Toplam	138					

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

Tablo 2 incelendiğinde erkek çalışma sıra ortalaması kadın katılımcı sıra ortalamasına göre düşük olsa bile bu istatistiksel olarak anlamlı fark oluşturmamaktadır. Bu nedenle bilgi güvenliği farkındalığı, cinsiyet değişkenine göre anlamlı farklılık göstermemektedir ($p>0,05$). Çalışmanın kurum türüne göre bilgi güvenliği farkındalığı ile ilgili Mann Whitney U testi sonucu Tablo 3'de verilmiştir.

Tablo 3.

Kurum Türüne Göre Bilgi Güvenliği Farkındalığı İle İlgili Mann Whitney U Testi Sonucu

Kurum türü	n	Sıra ortalaması	Sıra toplamı	U	p	Anlamlı fark
Kamu kurumu	85	67,11	5704,5	2049,5	0,373	Yok
Özel sektör	53	73,33	3886,5			
Toplam	138					

Tablo 3 incelendiğinde kamu kurumunda çalışanların sıra ortalamasının özel sektöre göre daha düşük olsa bile bu istatistiksel olarak anlamlı fark oluşturmamaktadır. Bu nedenle bilgi güvenliği farkındalığı, kurum türü değişkenine göre anlamlı farklılık göstermemektedir (p>0,05).

Çalışmanın yaş grubuna göre bilgi güvenliği farkındalığı ile ilgili Kruskal Wallis H testi sonucu Tablo 4'te verilmiştir.

Tablo 4

Yaş Grubuna Göre Bilgi Güvenliği Farkındalığı İle İlgili Kruskal Wallis H Testi Sonucu

Yaş	n	Sıra ortalaması	ss	x^2	p	Anlamlı fark
20-29 yaş arası	50	64,01	0,81	1,90	0,592	Yok
30-39 yaş arası	60	74,48				
40-49 yaş arası	23	68,98				
50 ve üzeri	5	67,00				
Toplam	138					

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

Tablo 5 incelendiğinde yaş grupları arasında sıra ortalama değerleri yakındır. 20-29 yaş arası sıra ortalama değeri diğer yaş aralığındaki sıra ortalama değerlerine göre düşük olsa bile bu istatistiksel olarak anlamlı fark oluşturmamaktadır. Bilgi güvenliği farkındalığı, yaş değişkenine göre anlamlı farklılık göstermemektedir (p>0,05).

Çalışmanın öğrenim durumuna göre bilgi güvenliği farkındalığı ile ilgili Kruskal Wallis H testi sonucu Tablo 5'te verilmiştir.

Tablo 5

Öğrenim Durumuna Göre Bilgi Güvenliği Farkındalığı İle İlgili Kruskal Wallis H Testi Sonucu

Öğrenim Durumu	n	Sıra ortalaması	ss	x^2	p	Anlamlı fark
Lise	1	119,50	0.7	4,21	0,378	Yok
Ön Lisans	11	62,68				
Lisans	75	67,10				
Yüksek Lisans	46	71,24				
Doktora	5	94,50				
Toplam	138					

Tablo 5 incelendiğinde ön lisans mezun sıra ortalamasının diğer öğrenim durumundaki sıra ortalamalarına göre düşük olsa bile bu istatistiksel olarak anlamlı fark oluşturmamaktadır. Bilgi güvenliği farkındalığı, öğrenim durumu değişkenine göre anlamlı farklılık göstermemektedir (p>0,05).

Çalışmanın işyerinde çalışılan pozisyon göre bilgi güvenliği farkındalığı ile ilgili Kruskal Wallis H testi sonucu Tablo 6'da verilmiştir.

Tablo 6

İşyerinde Çalışılan Pozisyona Göre Bilgi Güvenliği Farkındalığı İle İlgili Kruskal Wallis H Testi Sonucu

Pozisyon	n	Sıra ortalaması	ss	x^2	p	Anlamlı fark
Yönetici	22	69,32	0,63	1,19	0,551	Yok
Teknik personel	81	72,19				
İdari Personel	35	63,39				
Toplam	138					

Tablo 6 incelendiğinde idari personel sıra ortalamasının diğer pozisyonların sıra ortalamalarına göre düşük olsa bile bu istatistiksel olarak anlamlı fark oluşturmamaktadır. Bilgi güvenliği farkındalığı, işyerinde çalışılan pozisyon durum değişkenine göre anlamlı farklılık göstermemektedir (p>0,05).

Çalışmanın bilgi güvenliği kavramının öğrendikleri kaynağa göre bilgi güvenliği farkındalığı ile ilgili Kruskal Wallis H testi sonucu Tablo 7'de verilmiştir.

Tablo 7

Bilgi Güvenliği Kavramının Öğrenildiği Kaynağa Göre Bilgi Güvenliği Farkındalığı İle İlgili Kruskal Wallis H Testi Sonucu

Kaynak	n	Sıra ortalaması	ss	x^2	p	Anlamlı fark
Akademik	38	72,82	0,65	1,48	0,686	Yok
Alınan eğitim	85	69,93				
Medya	12	60,33				
Çevredeki kişiler	3	52,00				
Toplam	138					

Tablo 7 incelendiğinde çevredeki kişiler sıra ortalamasının diğer kaynakların sıra ortalamalarına göre düşük olsa bile bu istatistiksel olarak anlamlı fark oluşturmamaktadır. Bilgi güvenliği farkındalığı, bilgi güvenliği kavramının öğrenildiği kaynak değişkenine göre anlamlı farklılık göstermemektedir (p>0,05).

Çalışmanın işyerinde eğitim/kurs verilme durumuna göre bilgi güvenliği farkındalığı ile ilgili Mann Whitney U testi sonucu Tablo 8'de verilmiştir.

Tablo 8

İşyerinde Eğitim/Kurs Verilme Durumuna Göre Bilgi Güvenliği Farkındalığı Hakkında Mann Whitney U Testi Sonucu

Grup	N	Sıra ortalaması	Sıra toplamı	U	p	Anlamlı fark
Evet	121	73,79	8928	510	0,001	Var
Hayır	17	39,11	663			
Toplam	138					

Tablo 8 incelendiğinde hayır cevabı verenlerin sıra ortalama değerinin evet cevabı verenlerin sıra ortalama değerine göre oldukça düşük olduğu görülmektedir ve bu fark istatistiksel olarak anlamlı fark oluşturmaktadır. Bilgi güvenliği farkındalığı, işyerinde eğitim/kurs verilme değişkenine göre anlamlı farklılık göstermektedir ($U= 510$, $p<0,05$).

Çalışmanın işyerinde eğitim/kurs verilme sıklığına göre bilgi güvenliği farkındalığı ile ilgili Kruskal Wallis H testi sonucu Tablo 9'da verilmiştir.

Tablo 9

İşyerinde Eğitim/Kurs Verilme Sıklığına Göre Bilgi Güvenliği Farkındalığı İle İlgili Kruskal Wallis H Testi Sonucu

Sıklık	n	Sıra ortalaması	ss	x^2	p	Anlamlı fark
Bir yıldan fazla	15	80,73	0,89	7,10	0,068	Yok
Yılda bir	28	51,38				
Altı ayda bir	58	61,72				
Üç ayda bir	20	57,58				
Toplam	121					

Tablo 9 incelendiğinde yılda bir eğitim/kurs verilme sıra ortalamasının diğer seçeneklerdeki sıra ortalamalarına göre düşük olsa bile bu istatistiksel olarak anlamlı fark oluşturmamaktadır. Bilgi güvenliği farkındalığı, işyerinden alınan eğitim/kurs verilme sıklık derecesi değişkenine göre anlamlı farklılık göstermemektedir ($p>0,05$).

Çalışmaya katılanların bilgi güvenliği farkındalığı hakkında işyerinden aldıkları eğitimin/kursun fayda derecesine göre Kruskal Wallis H testi sonucu Tablo 10'da verilmiştir.

Tablo 10

İşyerinden Alınan Eğitimin/Kursun Fayda Derecesine Göre Bilgi Güvenliği Farkındalığı İle İlgili Kruskal Wallis H Testi Sonucu

Fayda derecesi	n	Sıra ortalaması	ss	x^2	p	Anlamlı fark
Faydasız	5	30,8	0,74	16,96	0,001	Var
Kararsızım	10	38				
Faydalı	65	57,06				
Çok Faydalı	41	76,54				
Toplam	121					

Tablo 10 incelendiğinde verilen eğitimin/kursun fayda derecesine göre çok faydalın seçeneğinin sıra ortalamasının; faydalı, kararsızım ve faydasız seçeneklerinin sıra ortalamasına göre yüksek olduğu görülmektedir ve bu fark istatistiksel olarak anlamlı fark oluşturmaktadır. Bilgi güvenliği farkındalığı, işyerinde alınan eğitimin/kursun fayda derecesi değişkenine göre anlamlı farklılaşma göstermektedir ($p<0,05$). Verilen eğitim/kurs çok faydalı bulunmaktadır.

Çalışmanın işyerinde bilgi güvenliği politikasının bulunma durumuna göre bilgi güvenliği farkındalığı ile ilgili Mann Whitney U testi sonucu Tablo 11'de verilmiştir.

Tablo 11

İşyerinde Bilgi Güvenliği Politikasının Bulunma Durumuna Göre Bilgi Güvenliği Farkındalığı İle İlgili Mann Whitney U Testi Sonucu Sonucu

Grup	n	Sıra ortalaması	Sıra toplamı	U	p	Anlamlı fark
Evet	132	72,22	9533,5	36,5	0,000	Var
Hayır	6	9,58	57,5			
Toplam	138					

Tablo 11 incelendiğinde hayır cevabı verenlerin sıra ortalama değerinin evet cevabı verenlerin sıra ortalama değerine göre oldukça düşük olduğu görülmektedir ve bu fark istatistiksel olarak anlamlı fark oluşturmaktadır. Bilgi güvenliği farkındalığı, işyerinde bilgi güvenliği politikasının bulunma değişkenine göre anlamlı farklılaşma göstermektedir ($U= 36,5$, $p<0,05$). Çalışanların büyük çoğunluğunun işyerinde bilgi güvenliği politikası mevcuttur.

Çalışmanın işyerinin bilgi güvenliği politikasını uygulama derecesine göre katılanların bilgi güvenliği farkındalığı ile ilgili Kruskal Wallis H testi sonucu Tablo 12'de verilmiştir.

Tablo 12

İşyerinin Bilgi Güvenliği Politikasını Uygulama Derecesine Göre Bilgi Güvenliği Farkındalığı İle İlgili Kruskal Wallis H Testi Sonucu Sonucu

Uygulanma derecesi	n	Sıra ortalaması	ss	x^2	p	Anlamlı fark
Hiç uygulanmıyor	1	1	0,81	36,27	0,00	Var
Uygulanmıyor	4	9,75				
Kararsızım	12	45,96				
Uygulanıyor	52	56,84				
Oldukça uygulanıyor	69	87,59				
Toplam	138					

Tablo 12 incelendiğinde işyerinde bilgi güvenliği politikasının uygulanma derecesine göre oldukça uygulanıyor seçeneğinin sıra ortalamasının; uygulanmıyor, kararsızım ve uygulanıyor sıra ortalamasına göre daha yüksek olduğu görülmektedir ve bu fark istatistiksel olarak anlamlı fark oluşturmaktadır. Bilgi güvenliği farkındalığı, işyerinde bilgi güvenliği politikasının uygulanma derecesine değişkenine göre anlamlı farklılaşma göstermektedir ($p<0,05$).

5. Sonuç

Çalışmaya katılan erkekler (%76,1) kadınlardan (%24,9) 3/4 oranında daha fazladır. Türkiye İstatistik Kurumunun verilerine göre 2017 yılında kadın istihdam oranı (%28,9) erkek istihdam oranının (%65,6) yarısından daha azdır (TÜİK, 2018, s. 1). Ayrıca Bilişim Sanayicileri Derneğinin (TÜBİSAD) 2021 yılında yayınladığı "*Bilgi ve İletişim Teknolojileri Sektörü 2020 Pazar Verileri Raporuna* göre bu alanda çalışan kadın oranı %29'dur (TÜBİSAD, 2020, s. 90). Çalışmaya katılan kişilerin cinsiyet oranındaki farklılık; kadınların erkeklere oranla daha az çalışma hayatında yer alması ve bilişim alanında daha az istihdam edildiği için olduğu düşünülmektedir. Bu çalışmada, cinsiyet değişkenine göre bilgi güvenliği farkındalık düzeyinde anlamlı fark bulunmamıştır. Özdemir ve Uluyol'un (2021) kamu kurum hakkında bilgi güvenliği farkındalığı, Canoğulları'nın (2021) öğretmenlerin bilgi güvenliği farkındalığı, Ceylan'ın (2019) Türkiye için bilgi güvenliği algısının istatistiksel analizi hakkında çalışmaları mevcuttur. Bu çalışmalardan çıkan sonuçlar için cinsiyet değişkene göre bilgi güvenliği farkındalık düzeyi anlamlı fark göstermemektedir. Korkmaz'ın (2018) üniversite öğrencilerine yönelik internet ve veri güvenliği farkındalığı çalışmasında, erkek öğrencilerin veri güvenliği algısı kız öğrencilere göre daha yüksektir ve bu durum istatistiksel olarak anlamlı fark göstermektedir.

Bu çalışmada, yaş değişkenine göre bilgi güvenliği farkındalık düzeyinde anlamlı fark bulunmamıştır. Çelikçöp ve Yarar'ın (2019) İstanbul ilini kapsayan kalite yönetim direktörleri için bilgi güvenliği çalışması, Okul ve diğerlerinin (2018) Kuşadası'ndaki konaklama işletme yöneticilerine yönelik bilgi güvenliği farkındalığı hakkındaki çalışmaları mevcuttur. Bu çalışmalardan çıkan sonuçlar için yaş değişkenine göre bilgi güvenliği farkındalık düzeyi anlamlı fark göstermemektedir. Keser ve Yayla'nın (2021) FATİH Projesi uygulanan okullardaki öğretmenlerin bilgi güvenliği farkındalık düzeyini incelediği çalışmada, öğretmenlerin yaşları arttıkça bilgi güvenliği farkındalık seviyesinde düşüş olmuştur ve bu durum istatistiksel olarak anlamlı fark göstermektedir.

Çalışmaya katılan kişilerin kamu kurumu veya özel sektörde çalışmaları bilgi güvenliği farkındalığı hakkında anlamlı fark oluşturmamakla beraber alanyazında bu sonuca ilişkin bir çalışmayla karşılaşılmamıştır. Ayrıca bu çalışmada, tıpkı kurum türü değişkeninin bilgi güvenliği farkındalığında anlamlı bir fark oluşturmadığı gibi bilgi güvenliği kavramının öğrenildiği kaynak türü değişkenine göre de bilgi güvenliği farkındalığında anlamlı bir fark görülmemektedir ve bu değişken türüne göre alanyazında bir çalışmayla karşılaşılmamıştır.

Bu çalışmada, öğrenim durumu değişkenine göre bilgi güvenliği farkındalık düzeyinde anlamlı fark bulunmamıştır. Yılmaz ve diğerlerinin (2016) öğretmenler için dijital veri güvenliği farkındalığı çalışması ve Ceylan'ın (2019) Türkiye için bilgi güvenliği algısının istatistiksel analiz hakkında çalışmaları mevcuttur. Bu çalışmalardan çıkan sonuçlar için öğrenim durumu değişkene göre bilgi güvenliği farkındalık düzeyi anlamlı fark göstermemektedir. Oktay ve Çakır'ın (2012) ilköğretim öğretmenlerinin teknolojiyi kullanma ve teknolojiye yönelimleri hakkındaki çalışmasında, eğitim düzeyi arttıkça bilgi güvenliği farkındalığı yükselmiştir ve bu durum istatistiksel olarak anlamlı fark göstermektedir.

Bu çalışmada, çalışılan pozisyon değişkenine göre bilgi güvenliği farkındalık düzeyinde anlamlı fark bulunmamıştır. Okul ve diğerlerinin (2018) Kuşadası'ndaki konaklama işletme yöneticilerine yönelik bilgi güvenliği farkındalığı, Özaslan'ın (2019) özel bir hastaneye yönelik bilgi güvenliği ve mahremiyet korunmasına yönelik eğitim etkinliğini değerlendirdiği, Kurt'un (2019) sağlık sektöründeki bilgi işlem çalışanlarına yönelik çalışmaları mevcuttur. Bu çalışmalardan çıkan sonuçlar için çalışılan pozisyon değişkenine göre bilgi güvenliği farkındalık düzeyi anlamlı fark göstermemektedir. Eş ve Serdar'ın (2021) Ankara ili için siber saldırılara karşı KOBİ'lerin farkındalık düzeyini incelediği çalışmasında, pozisyon yükseldikçe kişilerin şifre değiştirme sürecinin kısaldığı ve bilgi güvenliği farkındalığı seviyelerinin arttığı ifade gözlemlenmiştir. Bu durum istatistiksel olarak anlamlı fark göstermektedir.

Bu çalışmada, katılımcıların işyerinde bilgi güvenliği farkındalığı hakkında eğitim/kurs almaları bilgi güvenliği farkındalık düzeylerinde anlamlı farka yol açmıştır. Yayla'nın (2018) FATİH Projesi uygulanan ve uygulanmayan okullardaki öğretmenlere yönelik bilgi güvenliği farkındalığı çalışmasında, bilgi güvenliği eğitimi alan öğretmenlerin diğer öğretmenlere göre daha yüksek farkındalık seviyesine sahip olduğu belirtilmiştir. Fakeh ve diğerlerinin (2012) akademik kütüphaneciler arasındaki bilgi güvenliği bilincin belirlendiği çalışmasında alınan bilgi güvenliği eğitimleri bilgi güvenliği farkındalık seviyesini anlamlı biçimde farklılaştırmaktadır. Shehri ve Clarke'n (2007) bilgi güvenliği bilinci ve kültürü çalışmasında, güvenlik alanında eğitim alanların bilgi güvenliği farkındalıkları yüksek olduğu ifade edilmiştir.

Bu çalışmada, işyerinde bilgi güvenliği farkındalığı hakkında eğitim/kurs verilme sıklık derecesi değişkeni göre bilgi güvenliği farkındalık düzeyinde anlamlı fark bulunmamıştır. Pattinson ve diğerlerinin (2017) bir Avustralya bankasında bilgi güvenliğinin yönetilmesi üzerine yaptıkları çalışmasında, konu hakkında eğitim verilme sıklığının bilgi güvenliği farkındalığına anlamlı bir etkisi olmadığı belirtilmiştir.

Bu çalışmada, katılımcıların işyerinde aldıkları bilgi güvenliği farkındalığı hakkındaki eğitimi/kursu faydalı bulma derecesi bilgi güvenliği farkındalık düzeyinde anlamlı fark oluşturmaktadır. Gökçearslan ve diğerlerinin (2021) ortaokul öğrencileri ile yaptığı çalışmada, bilişim teknolojileri dersinden alınan faydanın farkındalığı artırdığı belirtilmiştir. Yayla'nın (2018) FATİH Projesi uygulanan ve uygulanmayan okullardaki öğretmenlere yönelik bilgi güvenliği farkındalığı çalışmasında, alınan eğitim öğretmenler tarafından yeterli bulunmaktadır ve bu durum istatistiksel olarak anlamlı fark göstermektedir.

Bu çalışmada, katılımcıların işyerlerinde bilgi güvenliği politikasına sahip olması bilgi güvenliği farkındalık düzeyinde anlamlı fark oluşturmaktadır ve katılımcıların büyük çoğunluğu işyerlerinde bilgi güvenliği politikasına sahiptir. Yıldırım'ın (2006) bankalardaki operasyonel risk yönetimine yönelik uygulama çalışmasında, bankaların 3/2'sinin bilgi güvenliği politikasına sahip olduğu ve bu durumun risk yönetimi ve iç denetimi arttırdığı belirtilmiştir. Ayrıca katılımcıların işyerlerinde bilgi güvenliği politikasının uygulanma derecesine göre bilgi güvenliği farkındalık düzeyinde anlamlı fark oluşturmaktadır. Bilgi güvenliği politikasının var olması ve uygulanma derecesindeki artış çalışanların bilgi güvenliği farkındalık seviyesini de yükseltmektedir.

6. Tartışma ve Sonuç

Araştırmada elde edilen bulgular ile alanyazındaki çalışmalar da incelenerek çıkan sonuçlara bakıldığında bilgi güvenliği farkındalığını etkileyen birçok neden olabileceği görülmüştür. Yapılan bu çalışmada bilgi güvenliği farkındalığını, firmada/kurumda bilgi güvenliği politikasının olması ve politikanın uygulanması, bilgi güvenliği farkındalığı hakkında verilen eğitimin/kursun etkili olduğu görülmüştür. Burada verilen eğitimin/kursun verilme sıklığından ziyade fayda derecesine odaklanmak doğru olacaktır. Firma/kurum çalışanları kamu veya özel sektörde çalışsınlar aldıkları eğitim/kurs öğretim programının kapsamlı olması beklenmektedir. Kurum/Firmalarda bilgi güvenliği politikalarının uygulanma durumu denetlenmelidir. Ayrıca bilgi güvenliği farkındalığı kültürü oluşturmak için kamu veya özel sektör çalışanlarına konu hakkında nitelikli eğitim/kurs veya çeşitli bilinçlendirme faaliyetleri gerçekleştirilmelidir. Kısacası bilgi güvenliği farkındalığında; yaş, cinsiyet, çalışılan pozisyon, kavramın öğrenildiği kaynağın türü, kurum türü, öğrenim durumu, firma/kurumda alınan eğitim/kurs verilme sıklık derecesi değil firmaların çalışanları için uygulanabilir ve denetlenebilir bilgi güvenliği politikasına sahip olması ve uygulanması ile kapsamlı ve nitelikli bilgi güvenliği farkındalığına yönelik kurs verilme durumu ve kursun faydalı olma durumu anlamlı etkiye sahiptir.

Bu araştırmanın bazı sınırlılıkları vardır. Çalışma grubu gönüllü katılımla seçilmiş katılımcılardan oluşmaktadır. Bu durum seçim yanlılığına neden olmuş olabilir. Farklı araştırma grubunda çalışabilir. Ölçme aracı, gerçek yaşam durumu problemleriyle veya yerinde gözlemlemelerle desteklenebilir. İleride yapılacak araştırmalarda sunulan kurusun öğretim tasarımı ile ilgili deneysel çalışmaların yapılması önerilmektedir. Akran öğrenmesi, probleme dayalı öğrenme veya otantik öğrenme yöntemlerin bilgi güvenliği farkındalığına etkisi ile ilgili araştırmalar yürütülebilir. Kurs ortamının yanı sıra gönderilecek iletiler ile yaparak yaşayarak veya yerinde öğrenme olanakları sunulabilir.

Etik Beyannamesi

Bu araştırma, Gazi Üniversitesi Etik Komisyonu 22.02.21 tarihli 32674/03 sayılı kararı ile alınan izinle yürütülmüştür. Ayrıca araştırmaya katılan bireylere çevrimiçi onam (olur) yazısı imzalatılmış olup ölçeği geliştiren Cüneyt ÇATUK'dan yazılı izin alınmıştır.

Çıkar Çatışması ve Yazar Katkıları

Bu çalışmada çıkar çatışması yoktur ve finansman desteği alınmamıştır. Yazarlar makaleye eşit katkı sağlamış olduklarını beyan ederler.

7. Referanslar

Abbas, J., Mahmood, H. K. & Hussain, F. (2015). Information security management for small and medium-size enterprises. *Science International Lahore, 27*(3), 2393-2398.

Agari (2020). *Cyber intelligence division.* https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-geography-of-bec.pdf

Ağır, O. & Turhan, A. (2014). Demokratik toplumda bilginin önemi ve Bilgi Edinme Hakkı Kanunu. *İnönü Üniversitesi Hukuk Fakültesi Dergisi, 5*(2), 283-312.

Ahlfeldt, R. M., Spagnoletti, P., & Sindre, G. (2007*). Improving the information security model by using TFI.* H. S. Venter, M.M. Eloff, L. Labuschange, J. H. P. Eloff, & R. VonSolms (Eds.). *In IFIP International Information Security Conference*, *232*, 73-84.

Åhlfeldt, RM., Spagnoletti, P., Sindre, G. (2007). Improving the ınformation security model by using TFI. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R. (Eds). New *Approaches for Security, Privacy and Trust in Complex Environments*. *SEC 2007 IFIP International Federation for Information Processing,* 232. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-72367-9_7

Ateş, V., & Güneş, B. (2016). Üniversitelerde bilişim teknolojileri risk yönetimi başarısını etkileyen faktörler üzerine nitel bir araştırma: Ankara ili örneği. *Bilgi Dünyası*, *17*(1), 39-56.

Atılgan, D. (2006). İletişim teknolojileri çağında değişen bilgi hizmetleri. http://hdl.handle.net/20.500.12575/41426

Ballı, F. E. ve Önder, E. (2019) Çeşitli değişkenler açısından öğretmenlerin örgütsel yaratıcılık algılarının incelenmesi. D. Özdemir, A. Kış (Eds.). *14. Uluslararası Eğitim Yönetimi Kongresi Tam Metin Bildiri Kitabı*, 518-522. http://acikerisim.ssu.edu.tr/xmlui/handle/123456789/54089

Baran, S., & Şener, E. (2020). Örgütlerde bilgi güvenliğini etkileyen bir unsur: Örgütsel bilgi paylaşımı. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (41), 410-427.

Barrett, N. (2003). Penetration testing and social engineering hacking the weakest link. *Information Security Technical Report*, *4*(8), 56-64.

Box, D., & Pottas, D. (2013). Improving information security behavior in the healthcare context. *Procedia Technology*, *9*, 1093-1103.

Boyacı, M., Benzer, R., & Ciylan, B. (2016). Siber güvenlik ve yapay sinir ağları yaklaşımıyla bir değerlendirme. V. Tecim, C. Aydın, & Ç. Tarhan (Eds.) *3. Uluslararası Yönetim Bilişim Sistemleri Konferansı Bildiriler Kitabı*. 32-43.

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

Canoğulları, E. (2021). Öğretmenlerin bilgi güvenliği konusundaki farkındalıklarının incelenmesi. *Kalem Eğitim ve İnsan Bilimleri Dergisi, 11*(2), 651-679. https://doi.org/10.23863/kalem.2021.219

Ceylan, H. (2019). *Türkiye'de bilgi güvenliği algısının istatistiksel analizi* (Yayın No. 607137) [Yüksek lisans tezi, İstanbul Üniversitesi]. YÖK Tez Merkezi.

Cherdantseva, Y. ve Hilton, J. (2013). A reference model of information assurance and security. *2013 International Conference on Availability, Reliability and Security*, 546- 555. https://doi.org/10.1109/ARES.2013.72

Choi, P. & Han, S. (2015). Effects of the recognition of business information protection activities in ranks on leaks of industrial secretes. *Journal of the Society of Disaster Information*, *11*(4), 475-486.

Cisco (2020). *2020 Annual report: Powering an inclusive future for all.* https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2020.pdf

Colwill, C. (2009). Human factors in information security: The insider threat: Who can you trust these days?. *Information Security Technical Report*, *14*(4), 186-196.

Çakmak, T., & Külcü, Ö. (2011). Kurumsal içerik yönetimi bileşenlerinin bir savunma sanayii organizasyonu örneğinde değerlendirilmesi. *Bilgi Dünyası*, *12*(2), 263-279.

Çalıkuşu, F., Karamehmet, B. & Denizci, Ö. M. Bilgi Güvenliği Yönetim Sistemi kapsamında risk yönetimi modeli. 1-8.

Çatuk, C. (2018). *Siber riskler karşısında KOBİ'lerin bilgi güvenliği farkındalıklarını ölçen bir ölçek geliştirme: Gaziantep örneklemi* (Yayın No. 498775) [Doktora tezi, Hasan Kalyoncu Üniversitesi]. YÖK Tez Merkezi.

Çelikçöp Ç. & Yarar O. (2019) Kalite yönetim direktörlerinin bilgi güvenliği farkındalığı: İstanbul ili örneği. *Sağlıkta Performans ve Kalite Dergisi*, *17*(2), 29-48.

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., & Gümüşgül, O. (2016). Gelecek zaman algısı: Beden eğitimi ve spor yüksekokulu öğrencilerine yönelik bir çalışma. *İstanbul Üniversitesi Spor Bilimleri Dergisi*, 6(1), 10-20.

Derin, M. A. & Gençoğlu, M. T. (2020). Ortaokul öğrencilerinin bilgi güvenliği farkındalığı. *Savunma Bilimleri Dergisi*, (38), 159-181.

Desman, M. B. (2001). *Building an information security awareness program* (1st ed.). CRC Press.

Dilek, S. (2016). Enformasyon ve bilgiye dayalı yeni ekonomi. *Kastamonu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *11*(1), 87-91.

Fakeh, S. K., Zulhemay, M. N., Shahibi, M. S., & Zaini, J. A. (2012). Information security awareness amongst academic librarians. *University Technology MARA*, *8*(3), 1723- 1735.

Fourkas, V. (2004). What is 'cyberspace'?. *WACC Media Development 2007/1: Fundamentalisms Revisited.*

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

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

Gökçearslan, Ş.ve Sarıtepeci, M. (2021). Nesnelerin internetinin eğitim boyutu. H. Çakır, Ç. Uluyol (Eds.). *Nesnelerin İnterneti Kuramdan Uygulamaya.* (s. 351-366). Nobel Akademik Yayıncılık.

Hai-Jew, S. (2019). The electronic hive mind and cybersecurity: Mass-scale human cognitive limits to explain the "weakest link" in cybersecurity. C, Bryan, & A. Piekarz (Eds.), *Global cyber security labor shortage and international business risk.* (s. 206-262). IGI Global.

Henkoğlu, T., & Özenç Uçak, N. (2012). Elektronik bilgi güvenliğinin sağlanması ile ilgili hukuki ve etik sorumluluklar. *Bilgi Dünyası*, *13* (2), 377-396.

IHS Markit (2017). *The Internet of Things: A movement, not a market*. https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

Jonsson, E. (2006). Towards an integrated conceptual model of security and dependability. *First International Conference on Availability, Reliability and Security.* 1-8. 10.1109/ARES.2006.138

Kalaycı, Ş. (2008). *SPSS uygulamalı çok değişkenli istatistik teknikleri* (3. baskı). Ankara: Asil Yayın Dağıtım.

Karakülah, Ü. H. (2006). *'Basit Rastgele Örnekleme Yönteminde Oransal Tahmin Ediciler* (Doctoral dissertation, Yüksek Lisans Tezi, Hacettepe Üniversitesi Fen Bilimleri Enstitüsü, Ankara).

Karasar, N. (2008). *Bilimsel araştırma yöntemi: kavramlar, ilkeler, teknikler* (18. basım). Nobel Yayın Dağıtım.

Keser, H., & Yayla, H. G. (2021). FATİH Projesi uygulanan okullardaki öğretmenlerin bilgi güvenliği farkındalık düzeylerinin incelenmesi. *Milli Eğitim Dergisi*, *50*(229), 9-40.

Keertikumar, M., Shubham, M., & Banakar, R. M. (2015). Evolution of IoT in smart vehicles: An overview. *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 804-809.

Konacaklı, E. (2019). *Ulusal güvenlik için blokzinciri tabanlısiber güvenlik modeli.* [Yüksek lisans tezi, Eskişehir Teknik Üniversitesi]. YÖK Tez Merkezi.

Korhan, S. (2017). Siber Uzayda aktör-güç ilişkisi. *Cyberpolitik Journal, 2*(4), 75-104.

Korkmaz, E. V. (2018). Üniversite öğrencilerinin internet ve veri güvenliği farkındalıkları. *Journal of Social And Humanities Sciences Research (JSHSR)*, *5*(25), 2222-2229.

Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840-847.

Kurt, S. G. (2019). *Bilgi güvenliğinin bilgi işlem çalışanları tarafından değerlendirilmesi sağlık sektöründe bir çalışma.* [Doktora tezi, Marmara Üniversitesi]. YÖK Tez Merkezi.

Lineberry, S. (2007). The human element: The weakest link in information security. *Journal of Accountancy*, *204*(5), 44.

McCumber, J. (1991). Information systems security: A comprehensive model. J. R. McCumber (Ed.). *In Proceedings 14th National Computer Security Conference*. 328-337.

Mears, L., & Von Solms, R. (2004). Corporate information security governance: A holistic approach. *Paper presented at the ISSA*. 2-11

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, *79*(119), 119-158.

Nunnally, J. C. (1975). Psychometric theory: 25 years ago and now. *Educational Researcher*, *4*(10), 7-21.

Oktay, S., & 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: Türkiye.

Okul, T., Şimşek, G., Hafçı, B., & Barış, Z. Bilgi güvenliği farkındalığı: Kuşadası'ndaki konaklama işletmesi yöneticileri üzerine bir uygulama. *Uluslararası Türk Dünyası Turizm Araştırmaları Dergisi*, *3*(2), 189-201.

Özaslan, G. (2019). *Bilgi güvenliği ve mahremiyetin korunmasına yönelik eğitimin etkilerinin değerlendirilmesi: Bir özel hastane uygulaması*. [Doktora tezi, Marmara Üniversitesi]. YÖK Tez Merkezi.

Özdemir, A., & Uluyol, Ç. (2021). Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, *25*(3), 649-666.

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.

Öztemiz, S., & Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. *Bilgi Dünyası*, *14*(1), 87-100.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2017). Managing information security awareness at an Australian bank: A comparative study. *Information & Computer Security*.

Pfleeger, C. P. (1997). The fundamentals of information security. *IEEE Software*, *14*(1), 15-16.

Ponemon Instıtue (2018). *Cyber intelligence division.* http://www.opus.com/2018-ciso-survey-ponemon-institute/

Röhrig, S. (2003). *Using process models to analyse it security requirements*. [Yayımlanmamış doktora tezi, Zürich Üniversitesi]
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.86.1352&rep=rep1&type=df

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

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177-191.

Suleymanova, G. (2015) *Betimsel istatistik ve histogram karma metodu,* (Yayın No. 614777) [Yüksek lisans tezi, Kırgızistan-Türkiye Manas Üniversitesi]. YÖK Tez Merkezi.

Sumathi, A. & Sundaram, B. V. (2015). An ANN approach in ensuring CIA triangle using an energy-based secured protocol E-AODV for enhancing the performance in MANETS. *Indian Journal of Science and Technology*, *8*(34), 1-10.

Şen, Ş., & Yerlikaya, T. (2013). ISO 27001: Kurumsal Bilgi Güvenliği Standardı. M. A., U. Çağlayan, E. Derman, A. Özgit, M. Topakcı, R. Uyar, O. Oral, Ş. Akbunar, T. F. Kasalak, E. Sezgin, F, Yücel, H. Akar, & U. Ercan (Eds.). *XV. Akademik Bilişim Konferansı*, 677-681.

Şimşek, Y., & Altınkurt, Y. (2009). Endüstri meslek liselerinde görev yapan öğretmenlerin okul müdürlerinin iletişim becerilerine ilişkin görüşleri. *Akademik bakış*, *17*, 1-16.

Taner, E., & Kılıç, İ. (2019). Güvenlik güçlerinin bilgi güvenliği farkındalığını belirlemeye yönelik bir araştırma. *Güvenlik Bilimleri Dergisi*, *8*(2), 253-269 https://doi.org/10.28956/gbd.646321

Toprak, H. (2020). Medyada bilgi edinimi ve izlence alanı arasında kalmak. *Ağrı İbrahim Çeçen Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *6*(1), 321-332.

Tryfonas, T., Gritzalis, D. ve Kokolakis, S. (2000). A qualitative approach to information availability. S. Oing, & J. H. P. Eloff (Eds.). *In IFIP International Information Security Conference*, 37-47.

TÜBİSAD (2020). *Bilgi ve İletişim Teknolojileri Sektörü 2020 Pazar Verileri,* https://www.tubisad.org.tr/tr/images/pdf/tubisad_bit_2020_raporu_tr.pdf

TÜİK (2018), *İstatistiklerle Kadın 2018*, https://data.tuik.gov.tr/Bulten/Index?p=Istatistiklerle-Kadin-2018-30707

Van Niekerk, JF (2005). *Establishing an information security culture in organizations: An outcomes-based education approach*. [Yayımlanmamış doktora tezi, Nelson Mandela Metropolitan Universitesi].

Varlı, B. ve Uluçınar Sağır, Ş. (2019). Araştırma sorgulamaya dayalı öğretimin ortaokul öğrencilerinin fen başarısı, sorgulama algısı ve üstbiliş farkındalığına etkisi. *Gazi University Journal of Gazi Educational Faculty (GUJGEF)*, 39(2), 703-725.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102.

Whitman, M. E., & Mattord, H. J. (2021). Principles of information security.*Cengage learning*.

Wilder, C. (2019). *Assessing the presence of mindfulness within cyber and non-cybersecurity groups.* (27736867) [Doktora Tezi, Nova Southeastern University]. ProQuest Dissertations & Theses Global.

Yayla, H. G. (2018). *FATİH projesi uygulanan ve uygulanmayan okullardaki öğretmenlerin bilgi güvenliği farkındalığının incelenmesi* (Yayın No. 515405) [Yüksek lisans tezi, Ankara Üniversitesi]. YÖK Tez Merkezi.

Yenal, Ü. (2009). Bilgi toplumunun tarihçesi. *Tarih Okulu Dergisi*, *V*, 123-144.

Yeniman Yıldırım, E. Y. (2018). Bilişim sistemlerine yönelik siber saldırılar ve siber güvenliğin sağlanması. *Mesleki Bilimler Dergisi (MBD)*, *7*(2), 24-33.

Yıldırım, H. (2006). *Bankalarda operasyonel risk yönetimi ve bir uygulama* (Yayın No. 191970) [Doktora tezi, Marmara Üniversitesi]. YÖK Tez Merkezi.

Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education*, *6*(2), 26-45.

Yoccoz, N. G. (1991). Use, overuse, and misuse of significance tests in evolutionary biology and ecology. *Bulletin of the Ecological Society of America,* 72(2), 106-111.