# Çalışanların Bilgi Güvenliği Önlemlerine Dair Tutumları: Ampirik Bir Değerlendirme*

Nurgül Ecek[1] Ahmet Ferda Çakmak[2]

Başvuru/Received: 10/03/2022 Yayın/Online Published: 20/10/2022
Kabul/Accepted: 02/05/2022

**Özet**

Bilgi çağı bilgi güvenliğini, hepimiz için önemli bir endişe kaynağı haline getirmiştir. Kurum ve kuruluşlar bilgi güvenliğini sağlamak için güvenlik teknolojilerini sürekli iyileştirerek teknik açıklarını azaltmaya çalışırken bilgi güvenliğine yönelik tehditler de hedef, etki alanı ve kullanılan teknikler açısından sürekli evrilerek insan unsuruna odaklanmaya başlamıştır. Çalışanlar, sosyal mühendislik ve dikkatsiz kullanıcı davranışları nedeni ile kurum ve kuruluşlarda en önemli güvenlik tehditlerinden sorumlu olarak gösterilmektedir. Ancak gerçek davranışları tahmin etmede etkili olduğu kabul edilen tutumun çalışanların bilgi güvenliği önlemlerini kabulü ve onların kullanımı üzerine etkisi hakkında çalışma eksikliği hissedilmektedir. Bu çalışmada çalışanların bilgi güvenliği önlemlerine dair tutumları Teknoloji Kabul Modeli (TKM) ile açıklanmaya çalışılmıştır. Bu amaçla Zonguldak'da 1490 kamu çalışanına anket uygulanmıştır. Teorik öngörüye de uygun olarak, algılanan fayda ve algılanan kullanım kolaylığının tutum üzerinde istatistiksel olarak anlamlı bir etkisi olduğu görülmüştür. Ayrıca bilgi güvenliği farkındalığının bazı alt boyutlarının algılanan fayda, algılanan kullanım kolaylığı ve tutum üzerinde kısmen anlamlı bir etkisi olduğu sonucuna ulaşılmıştır.

**Anahtar Kelimeler:** bilgi güvenliği önlemleri, tutum, teknoloji kabul modeli
**JEL Sınıflandırması:** M15, M19

# Employee Attitudes Towards Information Security Measures: An Empirical Assessment

**Abstract**

Information age has made information security an essential concern for us all. While institutions and organizations focus on reducing technical vulnerability by continuously improving security technologies, threats to information security have started to focus on the human element by constantly evolving in terms of target, domain and techniques used. Employees are shown to be responsible for the most critical security threats due to social engineering and careless user behavior. However, there is a lack of studies on the effect of the attitude, which is considered to be effective in predicting real behaviors, on the acceptance and use of information security measures by employees. The present study explores and tries explain employees' attitudes towards information security measures through the Technology Acceptance Model (TAM). For this purpose, a survey was conducted on 1490 public employees in Zonguldak. As predicted in theory, the results have shown that perceived usefulness and ease of use have a statistically significant effect on attitude. In addition, some subdimensions of information security

* Bu çalışma Nurgül ECEK'in Prof. Dr. Ahmet Ferda ÇAKMAK danışmanlığı altında yürütülen "Çalışanların Bilgi Güvenliği Önlemlerine Dair Tutumlarının İncelenmesi: Zonguldak İli Örneği" isimli doktora tezinden türetilmiştir.

[1]Zonguldak Bulent Ecevit University, Graduate School of Social Sciences, nurgulecek67@gmail.com
[2]Zonguldak Bulent Ecevit University, Faculty of Economics and Administrative Sciences, cakmak@beun.edu.tr

awareness partially have a statistically significant impact on perceived usefulness, perceived ease of use, and attide.

**Keywords:** information security measures, attitude, technology acceptance model

**JEL Classification:** M15, M19

## 1. Giriş

Örgütler, temel iş süreçlerinin oluşturulması, yürütülmesi ve sürekliliğinin sağlanmasında neredeyse tamamen bilgi teknolojilerine bağımlı hale gelmiştir. İşletmeler, yöneticilerin daha iyi kararlar almasına veya iş süreçlerinin iyileştirilmesine yardımcı olan bu sistemlere önemli yatırımlar yapmaya başlamışlardır (Laudon & Laudon, 2011, s. 12). Bilgi teknolojilerinin gelişmesi ve bu teknolojilere erişilebilirliğin artması sonucunda bilgi güvenliği önemli bir endişe kaynağı haline gelmiştir (Antoniou, 2015, s. 7; Koza, 2008, s. 411). Güvenlik teknolojilerinin sürekli olarak iyileştirilmesi ve daha iyi teknolojilerin geliştirilmesi teknik açıkları azaltıcı bir etki yaratmasına rağmen, istismar yöntemlerinin de insan unsuruna daha fazla odaklandığı dikkat çekmektedir (Mitnick & Simon, 2005, s. 4). Çalışanlar, bilgi sistemleri kullanımında üstlendikleri roller gereği, kuruluşların en önemli varlıkları olarak kabul edilmektedir (Merhi, 2014, s. 2). Ancak, kuruluşlarda meydana gelen güvenlik ihlallerinin de büyük çoğunluğunun mevcut çalışanlardan kaynaklandığı belirtilmektedir (Dhillon & Backhouse, 2000, s. 127). Benzer şekilde, çalışanların en önemli güvenlik tehditlerinden sorumlu oldukları ifade edilmektedir (İleri, 2018, s. 23). Birçok şirket bilgi kaybı yaşadığında para, müşteri, pazar, zaman, itibar kayıpları ve çeşitli cezai yaptırımlar gibi olumsuz sonuçlarla karşılaşabilmekte ve söz konusu şirketlerin bu kayıpları yerine koyabilmeleri ise çok yüksek maliyetler getirebilmektedir (Eminağaoğlu & Gökşen, 2009, s. 3; Yurtsever, 2013; Çatuk, 2018, s.110). Kurum ve kuruluşların varlıklarını sürdürebilmesi için bu tehditlerin farkında olmaları ve gerekli önlemleri almaları zorunludur.

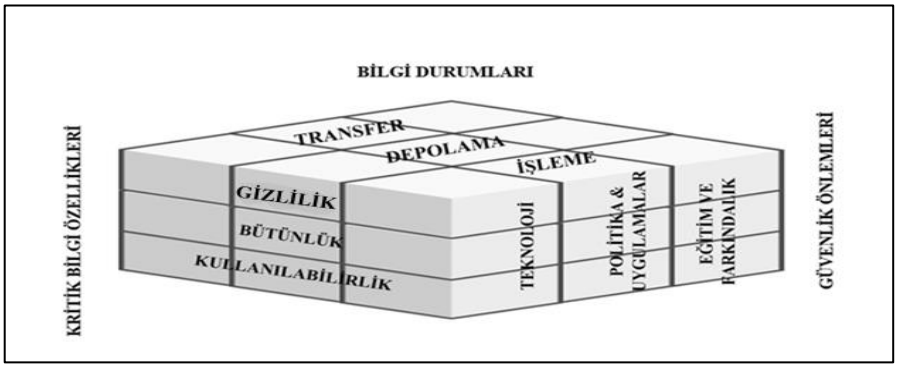
Gerçek davranışı tahmin etmede etkili olduğu düşünülen tutumun, bilgi sistemlerinin güvenliğine yönelik tedbir ve araçların kabulü ve kullanımı üzerindeki etkisi konusunda çalışma eksikliği hissedilmektedir. Bu amaçla bilgi sistemlerinin benimsenmesinde kullanılan Teknoloji Kabul Modeli (TAM) çerçevesinde çalışanların bilgi güvenliğine yönelik tutumlarının incelenmesi amaçlanmaktadır. Böylece çalışanların bilgi güvenliği önlemlerini benimseyip benimsemeyeceklerinin tahmin edilebileceği varsayılmaktadır.

## 2. Bilgi Güvenliği

Bilgi güvenliği genellikle bilginin gizlilik, bütünlük ve kullanılabilirliğinin sağlanması olarak tanımlanır. Diğer bir ifade ile bilginin yetkisiz erişime, kullanıma, ifşa edilmeye, bozulmaya, değiştirilmeye ve imha edilmeye karşı korunmasıdır (Raggad, 2010, s. 116; Peltier, 2001, s. 266).

McCumber (1990), bilgi güvenliğine yönelik çok boyutlu ve kapsamlı bir model önermiştir. Modele göre, güvence altına alınan merkezdeki bilgidir ve bilgi güvenliği, bilginin üç kritik özelliğinin sağlanması ile ilgilenmektedir. Şekil 1'de yer alan modelde, boyutlar sırası ile bilgi durumları, kritik bilgi özellikleri ve güvenlik önlemleri olarak gösterilmiştir. Modelin kullanım adımları; bilgi durumlarının tanımlanması, kritik bilgi özellikleri açısından değerlendirilerek güvenlik açıklarının belirlenmesi, bu güvenlik açıklarının minimize edilmesi için güvenlik

önlemlerinin alınması şeklinde özetlenebilir. Güvenlik önlemlerinde yer alan teknoloji ve politikanın, eğitim, öğretim ve farkındalık ile önemli derecede desteklenmesi gerektiği belirtilmektedir. Gizlilik özelliği, bilgilerin yetkisiz kişilere, işlemlere veya cihazlara karşı korunması, bütünlük özelliği, bilgilerin yetkisiz değişiklik veya imhaya karşı korunması ve kullanılabilirlik özelliği, bilgi güvenliği politikalarında belirtildiği biçimde bilgi kaynağına güvenilir erişimin sağlanması şeklinde açıklanabilir (Chen, 2012, s. 19-20; Raggad, 2010, s. 20).




**Şekil 1:** McCumber'in Bilgi Güvenliği Kavram Haritası

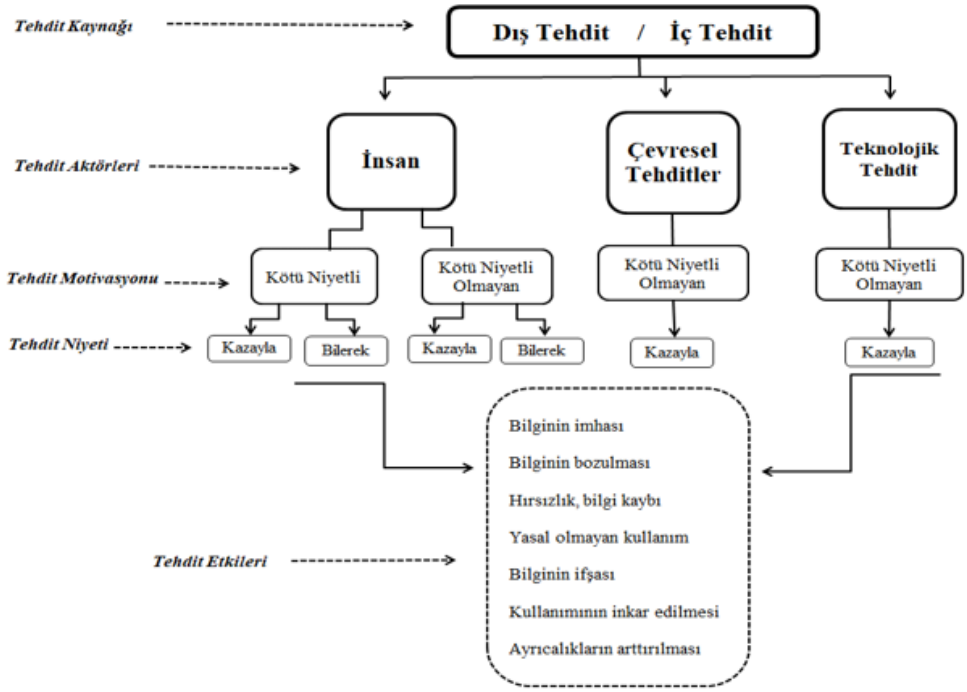
Kaynak: *J. R. McCumber (1990). Information Systems Security: A Comprehensive Model*. 14th National Computer Security Conference. Washington, s. 334.

Solms, bilgi güvenliğinin gelişimini belirli eğilimler açısından değerlendirerek beş dalga şeklinde sınıflandırmıştır. İlk dalgayı, 80'lerin başına kadar teknik yaklaşım oluşturmuştur. Bu yaklaşımda, bilgi güvenliğini sağlamak için parola, kimlik, erişim kontrol listeleri vb. önlemlerin etkili olacağı düşünülmüştür. İnternet ve e-ticaretin yaygınlaşması ile ortaya çıkan ikinci dalga olan yönetim yaklaşımında, üst yönetim sürece katılmış, konuyla ilgili politika ve prosedürler hazırlanmış ve hazırlanan raporlar yönetime sunulmuştur. Üçüncü dalga olan kurumsallaşma yaklaşımında ise standardizasyon, uluslararası sertifikasyon, şirket aracılığı ile bilgi güvenliği kültürünün geliştirilmesi, sürekli ve dinamik ölçümler yapılması vb. önemli gelişmeler yaşanmıştır (Solms, 2000, s. 615-616). Dördüncü dalga olan yönetişim yaklaşımında, farkındalık, paydaşların ilgili tüm politika, prosedür ve standartlara uyumunun sağlanması şeklinde teknik olmayan konulara da yer verilmiştir (Solms, 2006, s. 168). Son dalga olan siber yaklaşımda, zararlı yazılım, oltalama vb. tekniklerle işlenen suçların önlenebilmesi için güvenlik uygulayıcılarının her zaman profesyonel şekilde hareket etmesi gerektiği ve internet tabanlı sistemlerin güvensizliğe karşı uyarıda bulunabilmesi gerekliliği üzerinde durulmuştur (Solms, 2010, s. 5, 7).

Politika ve prosedürlere dayanarak tehditlerin ve alınacak önlemlerin farklılaştığı günümüzde IoT (nesnelerin interneti) (Hernandez, 2021; Corallo, Lazoi, Lezzi, & Luperto, 2022; Koohang, Sargent, Nord, & Paliszkiewicz, 2022; Matney, 2022), bulut (Anderson, 2021; Vargas Moya, 2021; Arshinskiy & Shurkhovetsky, 2022) ve güvenlik ile tehditlere ilişkin kullanıcı farkındalığı ve davranışları (Ngufor, 2020; Tientcheu, 2021; Rome, 2021; Herath, Khanna, & Ahmed, 2022; Chetioui, Bah, Alami, &Bahnasse, 2022) üzerine çalışmalar mevcuttur.

## 3. Güvenlik Tehditlerinin Sınıflandırılması

Bilgi güvenliğine yönelik tehdit kavramı, bilgilerin açıklanması, değiştirilmesi, imha edilmesi ya da kritik hizmetleri servis dışı bırakması aracılığı ile bir kuruluşa zarar verme potansiyeli bulunan herhangi bir durum ya da olay olarak tanımlanabilir (Wright, 2008, s. 28). Bu tehditlere doğal afetler, kazalar, kullanıcı hataları ya da kötü niyetli davranışlar yol açabilmektedir (Turan, 2019, s. 145). Tehditlerin sınıflandırılması, tanımlanması ve özelliklerinin anlaşılması, bilginin korunması için uygun ve etkili tedbirlerin alınması açısından oldukça önemlidir (Jouini, Rabai, & Aissa, 2014, s. 490). Literatürde tehditlere ilişkin farklı sınıflandırmalar yer almaktadır. Genel olarak tehditler; kaynakları, ajanları, motivasyonları, niyetleri ve etkilerine göre sınıflandırmalar yapılmıştır (Loch, Carr, & Warkentin, 1992; Peltier, 2005; Güldüren, 2015; Rencber & Mete, 2016). Jouini vd. (2014) tarafından geliştirilen sırasıyla kaynak, ajan, motivasyon, niyet ve etki kriterlerine dayanan çok boyutlu model Şekil 2'de gösterilmiştir.




**Şekil 2:** Çok Boyutlu Bilgi Güvenliği Tehdit Sınıflandırması Modeli

**Kaynak:** M. Jouini, L. B. A. Rabai & A.B. Aissa (2014). Classification of Security Threats in Information Systems. 5th International Conference on Ambient Systems, Networks and Technologies, Belgium, 2-5 June, s. 493

Şekil 2'de yer alan modelde, ilk olarak tehdit kaynağına göre, iç ve dış tehditler şeklinde sınıflandırma yapılmıştır. İç tehditler, kişinin ağ üzerindeki hesabı ile ya da fiziksel olarak ağa erişimi ile örgüt işleyişine ilişkin eylem ya da hatası sonucu ortaya çıkabilmektedir. Dış tehditler ise örgüt dışındaki çalışanlar ya da kurumların bağlantılı ağlar, ortak ağlar ya da fiziksel saldırı yöntemi ile sistem ve ağlara yetkisiz erişimleri sonucu meydana gelmektedir. İkinci sınıflandırma olan tehdit aktörleri; insan, doğal afet ve teknolojik olmak üzere üçe ayrılmıştır. İnsan aktörüne bağlı tehditler, örgüt içindekiler veya hackerların eylemlerinden

kaynaklanmaktadır. Çevresel tehditler, insan dışındaki aktörlerden kaynaklanmakta olup doğal afetler de bu grubun içinde yer almaktadır. Teknolojik tehditler ise, malzeme üzerindeki fiziksel ve kimyasal işlemlerin etkisinden kaynaklanmaktadır. Üçüncü sınıflandırma olan tehdit motivasyonu ise, saldırganların bir sisteme saldırma amacı ve güdüsünün bulunmasını ifade eder, bu amaçlar, kötü amaçlı veya kötü amaçlı olmayan sonuçlara yol açabilmektedir. Kötü amaçlı saldırılar arasında; virüs, truva atları, solucanlar aracılığıyla örgüt sistemine zarar veren eylemler bulunmaktadır. Kötü amaçlı olmayan saldırılar ise güvenlik açıklarına neden olan ve hatalara izin veren zayıf güvenlik politikaları ve kontroller ile sisteme zarar vermeyi amaçlamayan çalışan duyarsızlığı sonucu ortaya çıkabilmektedir. Son olarak tehdit niyeti sınıflandırması, tehdide neden olan insanların niyetlerini temsil etmekte olup bilerek veya kazayla yapılan şeklinde ayrılmıştır. Tüm bu tehditlerin etkileri ise, bilginin imhası, bozulması, kaybı, ifşası, kullanımının inkar edilmesi, ayrıcalıkların kaldırılması, yasal olmayan kullanımı şeklinde belirtilmiştir. Bilgi güvenliğine yönelik tehditlerin daha iyi anlaşılması, uygun stratejilerin geliştirilmesini sağlayarak söz konusu tehditleri önleyecek veya etkilerini azaltacak kararlar alınabilmesini mümkün kılacaktır (Jouini, Rabai, & Aissa, 2014, s. 490-496). Tehditlerin kaynakları öngörülebilmesine rağmen saldırıların nereden geleceği tahmin edilememektedir. Söz konusu tehditler sadece şirketleri değil kamu kurumları ve ülke güvenliğini de tehdit edebilmektedir (Çatuk, 2018, s. 109). Bilgi güvenliği sorunları; bilgisayar suçları, gizlilik sorunları ve diğer sorunsal unsurlar olarak sınıflandırılabilir. Bilgisayar suçları; bilgisayar korsanlığı, siber hırsızlık, siber terörizm, siber savaş, yazılım korsanlığı, fikri mülkiyet hırsızlığı vb. içermektedir. Gizlilik sorunları arasında; internet gizliliği, mahremiyetin korunması ve sansür sayılabilir. Diğer sorunsal unsurlar ise nitelikli çalışan temini ve bilgisayar izleme şeklinde sıralanabilir (Laudon & Laudon, 2011; Marakas & O'Brien, 2013).

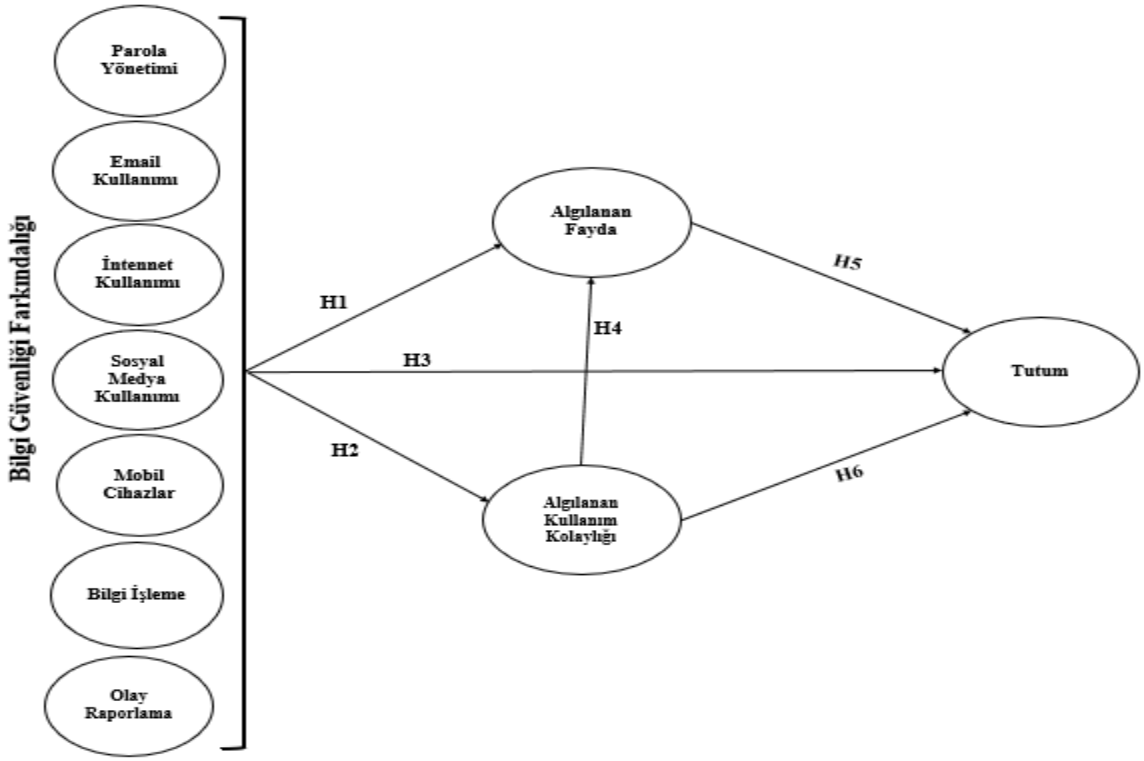
## 4. Güvenlik Yönetimi

Bilgi güvenliği yönetim sistemi (BGYS), tüm bilgi sistem süreçleri ve kaynaklarının doğruluğunu, bütünlüğünü ve güvenliğini sağlamak için sistemli, planlı, yönetilebilir, sürdürülebilir, dokumante edilmiş, yönetimce kabul görmüş uluslararası güvenlik standartları olan faaliyetlerin tümüdür (Ersoy, 2012, s.8). Kurumların bilgi varlıklarını koruması ve paydaşlarına güven vermesinin en iyi yollarından birinin BGYS'nin benimsenmesi olduğu belirtilmektedir (Erkan, 2006, s. 3). Etkili güvenlik yönetimi ile bilgi sistemlerindeki hatalar, ihlaller ve kayıplar minimize edilebilir. Sektörde önemli bir yere sahip olan Wang Global şirketine göre, güvenlik duvarları, ağ güvenlik protokolleri, yazılım araçları, saldırı tespit sistemleri, sanal özel ağlar, kriptografi, proxy sistemleri, yetkilendirme ve erişim kontrolü önemli güvenlik önlemleri olarak gösterilmektedir (Marakas & O'Brien, 2013, s. 596). Cherdantseva and Hilton (2013), güvenlik önlemlerini organizasyonel (strateji, prosedürler, politika, yönetişim, denetim), teknik (kriptografi, kimlik doğrulama, yetki), yasal (hukuk, sözleşmeler, anlaşmalar) ve insan odaklı olmak üzere dört boyutta sınıflandırmıştır. Şirketler çok iyi tasarlanan ve uygulanan güvenlik sistemlerine sahip olsalar dahi, yönetim ve kullanımın insan faktörüne bağlı olması nedeniyle (Karaoğlan Yılmaz, Yılmaz, & Sezer, 2014, s. 178), bilgi güvenliği sosyal ve örgütsel bir sorun olarak ele alınmaktadır (Dhillon & Backhouse, 2000, s. 126; Mitnick & Simon, 2005, s. 4). İnsanlar açgözlülük, panik, acelecilik gibi psikolojik faktörler ile, duyarsızlıkları, hataları ve kasıtlı veya kasıtsız davranışları nedeniyle güvenlik

açıklarına neden olabilmektedir (Gelişken, 2009, s. 65-69; Bulgurcu, Cavusoglu, & Benbasat, 2010, s. 525). Günümüzde güvenlik yönetiminin insan odaklı bir yaklaşım sergilediği görülmektedir.

## 5. Araştırma Modeli

Bilgi güvenliği önlemlerine yönelik tutum, TKM çerçevesinde ele alınmıştır.




**Şekil 3:** Araştırma Modeli

Şekil 3'te yer alan araştırma modeli, alt boyutlarına ayrılan bilgi güvenliği farkındalığı, TKM değişkenleri ile bilgi güvenliği önlemlerine yönelik tutum arasındaki ilişkileri yansıtmaktadır.

### 5.1. Tutum (TU)

Ajzen (1985) tarafından geliştirilen Planlı Davranış Teorisinde (PDT) bireyin bir davranışa yönelik tutumlarının, o davranışta bulunma niyetine yönlendiren unsur olduğu ileri sürülmektedir. Fishbein and Ajzen (1975), bireylerin belirli bir davranışı sergilemeleri için var olan tutumların bir ön koşul olduğunu belirtir iken, Lee vd. (2015), tutumun davranışa yönelik niyeti ve gerçekleşen davranışı belirlediğini öne sürmektedir. Bu araştırmada, çalışanların bilgi güvenliği önlemlerine dair tutumlarının bilgi güvenliği önlemlerini kullanıp kullanmadıklarının bir göstergesi olarak kullanılabileceği düşünülmektedir.

### 5.2. BGF (Bilgi Güvenliği Farkındalığı)

Kurumsal ve kişisel bilgi güvenliğinin sağlanabilmesi için teknik önlemlerin yanında kurum ve çalışanlarının da güvenlik bilincine sahip olması gerekir. Bilgi sistemleri, en zayıf halkanın sistem kullanıcıları olduğu ve bilgi güvenliği seviyesinin bu kullanıcılara bağlı olduğu bir zincir

olarak tasvir edilebilir (Güldüren, 2015, s. 4-5). Bilgi güvenliğinin ilk adımı olarak kabul edilen BGF (Hwang, Wakefield, Kim, & Kim, 2019, s.1), eğitim yoluyla öğretilen ve güvenlik politikaları ile desteklenen güvenlik uygulamaları ve politikalarına ilişkin bilgiyi ifade etmektedir (Lionel, 2020, s. 42). Parsons vd. (2017) tarafından BGF, bir kurumun çalışanlarının bilgi güvenliğinin önemini ve etkilerini ne ölçüde anladığının yanı sıra kurumun bilgi güvenliği politika ve prosedürlerine ne ölçüde uygun davrandığı şeklinde tanımlanmaktadır. Bu nedenle araştırma modelin ilk yapısını oluşturan BGF'e ilişkin hipotezler;

H1. Bir çalışanın bilgi güvenliği farkındalığının bilgi güvenliği önlemlerine dair fayda algısı üzerinde etkisi vardır.

H2. Bir çalışanın bilgi güvenliği farkındalığının bilgi güvenliği önlemlerine dair kullanım kolaylığı algısı üzerinde etkisi vardır.

H3. Bir çalışanın bilgi güvenliği farkındalığının bilgi güvenliği önlemlerine dair tutumu üzerinde etkisi vardır.

### 5.3. Algılanan Fayda (AF) ve Algılanan Kullanım Kolaylığı (AKK)

İnsanlar, işlerini daha iyi yapmalarına yardımcı olacağını düşündüklerinde bir uygulamayı kullanma eğilimindedir (Davis, 1989, s. 320). Bilgi sistemlerinin başarısını belirleyen en önemli faktör kullanıcı kabulüdür (Davis, 1993, s. 475). TKM, kullanıcıların teknoloji kabulünü ve kullanımını tahmin etmede yaygın olarak kullanılmaktadır (Gabbard, 2004; Kim, 2005; Young, 2010; Boone, 2011; Feistel, 2014). Davis (1989) tarafından geliştirilen TKM'ye göre, bir bireyin yeni teknoloji hakkındaki inançlarının iki belirleyicisi, algılanan fayda ve algılanan kullanım kolaylığıdır. Dolayısıyla algılanan fayda ve algılanan kullanım kolaylığının bilgi güvenliği önlemlerine dair tutumu etkileyeceği varsayılmaktadır.

H4. Bir çalışanın bilgi güvenliği önlemlerine dair kullanım kolaylığı algısının algılanan fayda üzerinde etkisi vardır

H5. Bir çalışanın bilgi güvenliği önlemlerine dair fayda algısının tutum üzerinde etkisi vardır.

H6. Bir çalışanın kullanım kolaylığı algısının tutum üzerinde etkisi vardır.

## 6. Yöntem

Araştırma, kamu kurumlarının içerdikleri kişisel veri boyutunun büyük olması ve daha katı bilgi güvenliği politikalarına sahip olmaları nedeniyle kamu çalışanları üzerinde yürütülen nicel bir çalışmadır. Araştırmanın evrenini Türkiye'de bilgi sistemlerini kullanarak görev yapan kamu çalışanları, örneklemini ise Zonguldak ilinde bilgi sistemlerini kullanarak görevini yapan kamu çalışanları oluşturmaktadır. Yıllık faaliyet raporları incelenerek ve ilgili kurum yetkilileri ile görüşülerek en çok çalışana sahip olan sağlık, eğitim, madencilik ve belediye sektörü çalışanları katılımcı olarak belirlenmiştir. Katılımcılara kurumlarından alınan iznin akabinde çevrimiçi hazırlanan anket formları gönderilmiştir. Ayrıca yeterli katılımın sağlanamadığı eğitim ve belediyecilik hizmetleri sektörüne fiziki anketler de dağıtılmıştır. 1490 geçerli anket elde edilmiştir. Araştırmanın sadece Zonguldak ilinde gerçekleştirilmesi, veri toplama sürecinin COVID-19 pandemi dönemine denk gelmesi ve katılımın gönüllülük esasına dayalı olması başlıca kısıtlardır.

Çalışmada bilgi güvenliği farkındalığı yapısı için Parsons vd. (2017) tarafından geliştirilen 7 alt boyut ve 63 maddeden oluşan 5'li likert tipi ölçek, algılanan fayda ve algılanan kullanım kolaylığı yapıları için Jones (2009) tarafından uyarlanan 11 maddeden oluşan 7'li likert tipi ölçek ve tutum yapısı için Bulgurcu vd. (2010) tarafından geliştirilen ve 4 maddeden oluşan 5'li likert tipi ölçek uyarlanarak kullanılmıştır.

Modelin analizi için PLS yol modeli kullanılmıştır. PLS, hem faktör modellerini hem bileşik modelleri işleyebilen, özyinelemeli ve özyinelemeli olmayan yapısal modelleri tahmin edebilen ve tam model uyum testleri gerçekleştirilebilen tam teşekküllü bir yapısal eşitlik modelleme yöntemi olarak ifade edilebilir (Henseler, 2017, s. 362; Henseler, Hubona, & Ray, 2015, s. 3). Araştırma, 9 gizil değişkenin ve aralarındaki ilişkilerin analiz edildiği karmaşık bir model üzerinde gerçekleştirilmiştir.

## 7. Bulgular

Bulgular, katılımcıların demografik özellikleri, uyum analizi, ölçeklerin güvenirlik ve geçerlik analizleri, bağımlı değişkenlerin belirleme katsayıları ve hipotez testlerinin analiz sonuçları başlıkları altında organize edilmiştir.

### 7.1. Tanımlayıcı İstatistiklerin Analizi

Katılımcıların %39'unun sağlık sektöründe, %33'ünün 30-39 yaş grubu aralığında yer aldığı, katılımcıların yarısından fazlasını erkeklerin oluşturduğu, yine katılımcıların yarısından fazlasının öğrenim durumunun lisans olduğu görülmektedir. Katılımcıların %33'ünün 0-9 yıl arası çalışma süresi grubunda bulunduğu ve %76'sının iş yerinde ortalama 1-6 saat aralığında bilgisayar kullandığı belirlenmiştir. Ayrıca fark analizleri yapıldığında sektörler açısından bir herhangi bir farklılık bulunmadığı anlaşılmıştır.

### 7.2. Uyum Analizi

Hu and Bentler (1999), standardize edilmiş kök ortalama kare artığın (SRMR) PLS'de yaklaşık model uyum kriteri olarak uygulanan tek ölçü olduğunu belirtmiştir. SRMR, modelin gözlenen korelasyon matrisi ile modelin ima edilen korelasyon matrisi arasındaki fark olarak ifade edilebilir ve Henseler vd. (2014), SRMR'yi modelin yanlış belirlenmesinin önelenebilmesinde kullanılabilecek uyum iyiliği kriteri olarak tanıtmıştır. Modeldeki SRMR değerinin literatürdeki ⩽,80 kriterini karşıladığı görülmektedir.

**Tablo 1:** Uyum indeksleri

| | Tahmini Model |
|---|---|
| SRMR | 0,058 |
| Chi-Square | 5.704.759 |

### 7.3.Geçerlilik ve Güvenilirlik

Yapıların, kendilerine atanan göstergeler tarafından ne kadar iyi ölçüldüğünün belirlenebilmesi için (Albers, 2010, s. 28) cronbach alfa ve bileşik güvenilirlik (CR) katsayıları incelenmiştir. Birleşim geçerliliği için faktör yükleri ve açıklanan ortalama varyans (AVE) değerleri

incelenmiştir. Ölçüm modelinin değerlendirilmesinde ilk kriter olarak faktör yüklerinin ⩾,70 olması önerilmektedir (Hair, Risher, Sarstedt, & Ringle, 2019, s. 8). Bilgi güvenliği farkındalığının alt boyutları olan parola yönetimi, email kullanımı, sosyal medya kullanımı, mobil cihazlar, bilgi işleme ve olay raporlama göstergelerinden bazıları ile internet kullanımının tüm faktör yükleri ,40-,70 değerleri arasında bulunmuştur. Hesaplamalar, faktör yükleri ,40-,70 arasında olan ifadelerin AVE veya CR değerleri referans değerin altında olanlar analiz dışı bırakılarak gerçekleştirilmiştir. Tablo 3'te gösterilen analiz sonuçlarına göre faktör yükleri ,589-,933 değerleri arasında hesaplanmıştır. Cronbach alfa katsayıları ,740-,946 değerleri arasında ve CR katsayıları ,853-,957 değerleri arasında bulunduğundan modelin içsel tutarlılığa sahip olduğu sonucuna ulaşılmıştır.

**Tablo 2:** Tanımlayıcı istatistikler, bileşik güvenilirlik (CR), and Cronbach alfa (CA) puanları

| YAPI | CR (CA) | AVE | Mean (SS) | TU | EK | Bİ | OR | MC | AKK | PY | AF | SMK |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **TU** | ,94 (,91) | ,79 | ,89 (.01) | **,89** | | | | | | | | |
| **EK** | ,86 (,76) | ,67 | ,82 (.02) | ,30 | **,82** | | | | | | | |
| **Bİ** | ,86 (,80) | ,56 | ,74 (.02) | ,40 | ,46 | **,75** | | | | | | |
| **OR** | ,87 (,81) | ,56 | ,75 (.02) | ,46 | ,37 | ,59 | **,75** | | | | | |
| **MC** | ,86 (,78) | ,60 | ,77 (.02) | ,41 | ,33 | ,61 | ,57 | **,78** | | | | |
| **AKK** | ,92 (,89) | ,70 | ,83 (.01) | ,44 | ,20 | ,27 | ,38 | ,34 | **,84** | | | |
| **PY** | ,85 (,74) | ,65 | ,81 (.04) | ,15 | ,19 | ,22 | ,18 | ,18 | ,09 | **,81** | | |
| **AF** | ,96 (,95) | ,79 | ,89 (.01) | ,49 | ,22 | ,38 | ,53 | ,42 | ,60 | ,17 | **,89** | |
| **SMK** | .86 (,74) | ,67 | ,81 (.02) | ,38 | ,30 | ,50 | ,49 | ,58 | ,33 | ,18 | ,43 | **,82** |

Not: Köşegen üzerindeki maddeler (kalın harflerle), AVE puanlarının karekökünü temsil etmektedir.

AVE tahmini, gizli bir yapının teorik olarak ilişkili olduğu gözlenen değişkenlerde açıklayabildiği ortalama varyans miktarı olup (Farrel, 2010, s. 324), kabul edilebilir AVE değerinin ⩾,50 olması gerektiği belirtilmektedir (Hair, Risher, Sarstedt, & Ringle, 2019, s. 9). Gizli değişkenlerin AVE değerlerinin ,553-,792 arasında değiştiği görülmüş olup, yapılar için birleşim geçerliliği kriterlerinin karşılandığı sonucuna ulaşılmıştır.

Ayrışım geçerliliği için, Fornell-Larcker (1981) kriter tablosunda köşegen hücrelerdeki AVE'nin karekökü, diğer gizli değişkenlerle olan korelasyonundan daha yüksek olmalıdır (Hulland, 1999, s. 200; Garson, 2016, s. 67; Henseler, 2017, s. 371). Ölçüm modelinde yer alan yapıların ayrışım geçerliliğine sahip olduğu sonucuna ulaşılmıştır.

Gözlenen değişkenlerin faktör yüklerinin istatistiksel anlamlılığını test etmek için orjinal verilerden çok sayıda alt örneklem alınarak modellerin tahmin edilmesini sağlayan, önyükleme adı verilen bir yeniden örnekleme tekniği kullanılmıştır (Hair, Hult, Ringle, & Sarstedt, 2014a, s. 201). İki uçlu bir test için t değerleri kritik değerden büyükse, katsayı belirli bir hata olasılığı ile istatistiksel olarak anlamlı kabul edilir, kritik değer 1,65 ve üzeri ise hata payının %10, 1,96 ve üzeri ise hata payının %5 ve 2,58 ve üzeri ise hata payının %1 olacağı belirtilmektedir (Hair,

Ringle, & Sarstedt, 2011, s. 145). Çalışmadaki tüm analizler için t istatistiği ve p değerlerinin anlamlılık düzeyi %95 olarak belirlenmiş olup t istatistiği sonuçlarının tüm gözlenen değişkenler için 1,96 eşik değerinin üzerinde gerçekleştiği, p değerlerinin referans alınan 0,05 eşik değerinin altında olduğu ve araştırma modelinin %95 güven aralığında anlamlı olduğu görülmüştür.

**Table 3:** Gizli değişkenler ve faktör yükleri

| Gizli Değişkenler | | Faktör Yükleri | Mean | Std.Sapma | t | p |
|---|---|---|---|---|---|---|
| **Parola Yönetimi** | PY4 | 0,804 | 0,8 | 0,035 | 23,029 | 0,000* |
| | PY5 | 0,807 | 0,808 | 0,038 | 21,166 | 0,000* |
| | PY6 | 0,812 | 0,808 | 0,034 | 24,117 | 0,000* |
| **Email Kullanımı** | EK5 | 0,807 | 0,807 | 0,022 | 36,115 | 0,000* |
| | EK6 | 0,843 | 0,842 | 0,017 | 51,043 | 0,000* |
| | EK7 | 0,812 | 0,812 | 0,021 | 38,259 | 0,000* |
| **Sosyal Medya Kullanımı** | SMK1 | 0,89 | 0,89 | 0,011 | 79,206 | 0,000* |
| | SMK2 | 0,902 | 0,901 | 0,008 | 108,39 | 0,000* |
| | SMK6 | 0,631 | 0,631 | 0,031 | 20,388 | 0,000* |
| **Mobil Cihazlar** | MC5 | 0,626 | 0,626 | 0,034 | 18,342 | 0,000* |
| | MC7 | 0,83 | 0,828 | 0,017 | 48,43 | 0,000* |
| | MC8 | 0,784 | 0,784 | 0,024 | 33,341 | 0,000* |
| | MC9 | 0,847 | 0,847 | 0,013 | 64,734 | 0,000* |
| **Bilgi İşleme** | Bİ5 | 0,726 | 0,725 | 0,022 | 33,084 | 0,000* |
| | Bİ6 | 0,668 | 0,668 | 0,027 | 24,718 | 0,000* |
| | Bİ7 | 0,802 | 0,801 | 0,016 | 49,901 | 0,000* |
| | Bİ8 | 0,75 | 0,75 | 0,019 | 40,282 | 0,000* |
| | Bİ9 | 0,772 | 0,772 | 0,019 | 39,776 | 0,000* |

*p<0,01 (%1 hata payı, %99 anlamlılık)

**Tablo 3:** (Devamı)

| Gizli Değişkenler | İfade | Faktör Yükleri | Mean | Std.Sapma | t | p |
|---|---|---|---|---|---|---|
| **Olay Raporlama** | OR1 | 0,796 | 0,796 | 0,015 | 52,047 | 0,000* |
| | OR2 | 0,696 | 0,695 | 0,023 | 30,313 | 0,000* |
| | OR3 | 0,803 | 0,803 | 0,015 | 55,298 | 0,000* |
| | OR5 | 0,675 | 0,675 | 0,024 | 28,112 | 0,000* |
| | OR9 | 0,771 | 0,771 | 0,014 | 54,402 | 0,000* |
| **Algılanan Fayda** | AF1 | 0,853 | 0,852 | 0,012 | 71,391 | 0,000* |
| | AF2 | 0,917 | 0,917 | 0,007 | 129,37 | 0,000* |
| | AF3 | 0,897 | 0,897 | 0,013 | 70,078 | 0,000* |
| | AF4 | 0,919 | 0,919 | 0,007 | 132,32 | 0,000* |
| | AF5 | 0,911 | 0,911 | 0,007 | 122,23 | 0,000* |
| | AF6 | 0,823 | 0,823 | 0,014 | 56,848 | 0,000* |
| **Algılanan Kullanım Kolaylığı** | AKK1 | 0,839 | 0,839 | 0,012 | 68,931 | 0,000* |
| | AKK2 | 0,915 | 0,915 | 0,006 | 148,24 | 0,000* |
| | AKK3 | 0,913 | 0,913 | 0,007 | 139,58 | 0,000* |
| | AKK4 | 0,877 | 0,877 | 0,011 | 78,427 | 0,000* |
| | AKK5 | 0,588 | 0,588 | 0,026 | 22,764 | 0,000* |
| **Tutum** | TU1 | 0,896 | 0,897 | 0,013 | 70,182 | 0,000* |
| | TU2 | 0,933 | 0,933 | 0,008 | 112,95 | 0,000* |
| | TU3 | 0,933 | 0,933 | 0,008 | 121,43 | 0,000* |
| | TU4 | 0,789 | 0,789 | 0,016 | 48,376 | 0,000* |

*p<0,01 (%1 hata payı, %99 anlamlılık)

### 7.4. Yapısal Model Sonuçları

Belirleme katsayısı olan R2 değeri, yapısal modelin değerlendirilmesinde en sık kullanılan ölçüdür ve modelin tahmin doğruluğunun bir göstergesidir (Hair, Sarstedt, Hopkins, & Kuppelwieser, 2014b, s. 113; Nitzl, 2016, s. 21). R2 değeri, dışsal değişkenlerin içsel değişkenler üzerindeki birleşik etkisini temsil eder. R2 değerlerinin kabul edilebilirliğinin model karmaşıklığı ve ilgili araştırma disiplinine bağlı olarak değiştiği belirtilmektedir (Hair, Sarstedt, Hopkins, & Kuppelwieser, 2014b, s.113, 175; Hair, Ringle, & Sarstedt, 2011, s. 147). Chin (1998) içsel gizli değişkenlerdeki R2 değerini 0,67 eşik değeri ve üzerindeki sonuçlar için "önemli", 0,33 eşik değeri ve üzerindeki sonuçlar için "orta" ve 0,19 eşik değeri ve üzeri için "zayıf" olarak tanımlamaktadır. Algılanan fayda ve tutum için R2 değerinin orta derecede önemli olduğu görülmüştür.

Araştırma modelinde iki veya daha fazla bağımsız değişkenin yüksek düzeyde ilişkili olması durumunda çoklu doğrusallık sorunu ortaya çıkmaktadır (Garson, 2016, s. 71). Uygun bir modelde VIF katsayıları için genellikle 4 eşik değeri olarak kabul edilirken bazı araştırmacılar daha esnek olan 5 eşik değerini kullanmaktadır (Garson, 2016, s. 71; Hair, Ringle, & Sarstedt, 2011, s. 145). VIF değerleri incelendiğinde değişkenler arasında çoklu doğrusal bağlantı sorunu olmadığı görülmüştür.

**Table 4:** VIF, $R^2$ Değerleri

| Yapılar | | VIF | R2 |
|---|---|---|---|
| Parola Yönetimi | Algılanan Fayda | 1,07 | 0,48 |
| Sosyal Medya Kullanımı | | 1,676 | |
| Olay Raporlama | | 1,863 | |
| Algılanan Kullanım Kolaylığı | | 1.219 | |
| Sosyal Medya Kullanımı | Algılanan Kullanım Kolaylığı | 1,648 | 0,178 |
| Mobil Cihazlar | | 2,066 | |
| Olay Raporlama | | 1,793 | |
| Email Kullanımı | Tutum | 1,314 | |
| Bilgi İşleme | | 2,12 | |
| Olay Raporlama | | 2,009 | 0,345 |
| Algılanan Fayda | | 1,929 | |
| Algılanan Kullanım Kolaylığı | | 1,592 | |

#### 7.4.1. Araştırma Hipotezlerinin Test Edilmesi

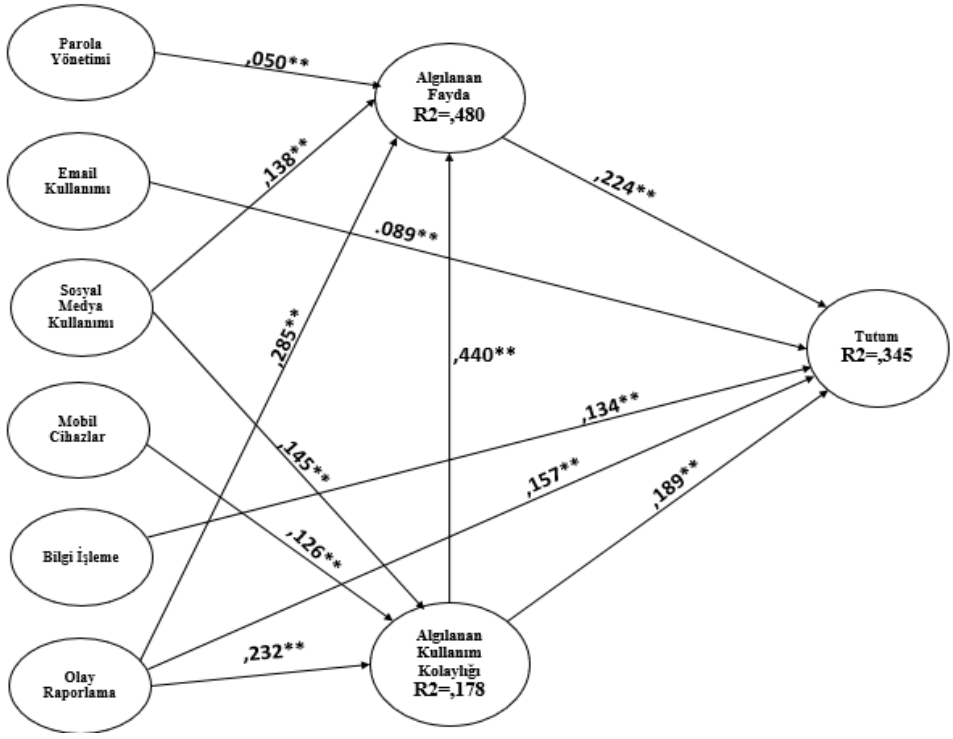
SmartPLS algoritması çalıştırılarak yeniden örnekleme metoduyla 5000 alt örneklem alınarak araştırmada öngörülen ilişkilerin model tarafından desteklenip desteklenmediğini gösteren "t istatistiği", yol katsayıları (Standardize β) and "p değerleri" incelenmiştir. t istatistiği

sonuçlarına göre “t” değeri 2,58 eşik değerinden büyük olan ve p<0,01 düzeyinde anlamlı sonuç veren ilişkiler Tablo 5’te gösterilmiştir.

**Table 5:** Yapısal Modelin Standardize β, t and p değerleri

| | Yapılar | | Std. β | Standart Deviation | t | p |
|---|---|---|---|---|---|---|
| BGF | Parola Yönetimi | Algılanan Fayda | 0,050 | 0,019 | 2,632 | 0,009* |
| BGF | Sosyal Medya Kullanımı | | 0,138 | 0,027 | 5,170 | 0,000* |
| BGF | Olay Raporlama | | 0,285 | 0,027 | 10,446 | 0,000* |
| Algılanan Kullanım Kolaylığı | | | 0,440 | 0,026 | 17,066 | 0,000* |
| BGF | Sosyal Medya Kullanımı | Algılanan Kullanım Kolaylığı | 0,145 | 0,032 | 4,598 | 0,000* |
| BGF | Mobil Cihazlar | | 0,126 | 0,032 | 3,919 | 0,000* |
| BGF | Olay Raporlama | | 0,232 | 0,033 | 7,041 | 0,000* |
| BGF | Email Kullanımı | Tutum | 0,089 | 0,028 | 3,188 | 0,001* |
| BGF | Olay Raporlama | | 0,157 | 0,030 | 5,333 | 0,000* |
| BGF | Bilgi İşleme | | 0,134 | 0,034 | 3,996 | 0,000* |
| Algılanan Fayda | | | 0,224 | 0,034 | 6,534 | 0,000* |
| Algılanan Kullanım Kolaylığı | | | 0,189 | 0,028 | 6,858 | 0,000* |

*p<0,01 (1% hata payı, 99% anlamlılık)




**Şekil 4:** Araştırma Modeli Sonuçları (** p<.001; anlamlı olmayan yollar gösterilmemiştir)

Önerilen ve doğrulanan hipotezlerin sonuçları Şekil 4'e gösterilmektedir.

## 8. Sonuç

Kamu çalışanlarının katılımıyla gerçekleştirilen araştırmadan elde edilen bulgular; BGF'nin bazı alt boyutları, TKM değişkenleri ve çalışanların tutumları arasında anlamlı ilişkilerin olduğunu göstermiştir.

BGF'nin bilgi güvenliği için merkezi bir aktör olduğu onaylanmıştır (McCormac et al., 2017; Grassegger & Nedbal, 2021). Al-Omari vd. (2012), BGF'nin güvenlik politikalarına uyum davranışlarını şekillendirmede etkili olduğunu ifade ederken Metalidou vd. (2014) ise BGF'nin insanın zaaflarından kaynaklanan güvenlik tehditlerini azaltmada anahtar bir rolü olduğunu belirtmiştir. Bu çalışma, BGF'nin algılanan fayda üzerinde istatistiksel olarak kısmen anlamlı pozitif yönde bir etkisi olduğunu göstermiştir. Çalışmamızın bulguları, Al-Omari vd. (2012) çalışmasının sonuçlarını destekler niteliktedir.

BGF sağlanırken, tüm çalışanların konuyla ilgili politika ve prosedürleri sıkıcı bulmaması, onları ekstra iş yükü olarak görmekten ziyade, kolay anlaşılır, açık ve basit olarak algılaması gerektiği belirtilmektedir (Eminağaoğlu, Uçar, & Eren, 2009b; Safa et al., 2015). Bu çalışmada BGF'nin algılanan kullanım kolaylığı üzerinde istatistiksel olarak kısmen anlamlı pozitif yönde bir etkiye sahip olduğu ortaya konulmuştur. Safa vd. (2015), BGF'nin kullanıcıların bilgi güvenliği ile ilgili bilinçli davranış sergilemeye yönelik tutumlarını olumlu yönde değiştirdiğini gözlemlerken, Bulgurcu vd. (2010), BGF'nin güvenlik politikalarına uyma konusundaki tutumlarını doğrudan ve dolaylı olarak etkilediğini ortaya koymuştur. Bu çalışmanın bulgularının Safa vd. (2015) ile Bulgurcu vd. (2010) bulguları ile uyumlu olduğu söylenebilir.

Jones (2010), algılanan fayda ile algılanan kullanım kolaylığı arasında istatistiksel olarak anlamlı pozitif bir ilişki bulunduğunu ortaya koymuştur. Bu çalışmada da algılanan kullanım kolaylığının algılanan fayda üzerinde pozitif yönde anlamlı bir etkisi olduğu ortaya çıkmıştır.

Özer vd. (2010), algılanan fayda ve algılanan kullanım kolaylığı değişkenlerinin bilgi teknolojisi kullanımına yönelik tutum üzerinde istatistiksel olarak anlamlı pozitif yönde bir etkiye sahip olduğunu ortaya koymuştur. Teo vd. (2008), algılanan fayda ve kullanım kolaylığının tutumun önemli belirleyicileri olduğunu ortaya çıkarmıştır. Bu çalışma da teorik öngörüye uygun olarak algılanan fayda ve algılanan kullanım kolaylığının tutum üzerinde istatistiksel olarak anlamlı pozitif yönde bir etkisi olduğunu ortaya çıkarmıştır.

Ampirik çalışmamız sonucunda modelin çalışanların bilgi güvenliği önlemlerine yönelik tutumlarını anlama ve açıklamada faydalı bir teorik model olduğu sonucuna ulaşılmıştır. Sonuçlar, algılanan fayda, algılanan kullanım kolaylığı ve bilgi güvenliği farkındalığının email kullanımı, bilgi işleme ve olay raporlama alt boyutlarının tutum üzerinde istatistiksel olarak anlamlı bir etkiye sahip olduğunu göstermiştir. Ayrıca teorik öngörü ile uyumlu olarak algılanan kullanım kolaylığının algılanan fayda üzerinde istatistiksel olarak anlamlı bir etkiye sahip olduğu görülmüştür. Bilgi güvenliği önlemlerine yönelik tutumun varyansı, önerilen modelin %35'ini açıklamaktadır.

Bilgi güvenliğinin artan bir ivme ile işletmecilik alanının önemli sorunsallarından bir olacağını öngörebilmekteyiz. Son yıllarda 4. Sanayi Devrimi ile hayatımıza giren IoT kavramı ve değer zincirinde yer alan bilgilerin entegrasyonunun, dijital dönüşüm sürecinde işletmeciliğin odağında olacağı ve işletmelerin hedeflerine ulaşmasında veri güvenliğinin kritik bir öneme sahip olacağı açıktır. Teknik ve sosyal bir varlık olan işletmelerin bilgi güvenliği sorunlarının disiplinler arası araştırmalarla daha iyi anlaşılması ve söz konusu sorunlara çözüm geliştirilmesi ihtiyacından hareketle, bu çalışma endüstriyelden akademik alana kadar dikkatlerin bu konuya odaklanmasını sağlayacaktır. Ayrıca bu çalışma, güvenlik önlemlerinin benimsenmesinde tutumun etkili olduğuna dair farkındalığı arttırarak bilgi güvenliği yönetimi süreci ile ilgili işletmelere katkı sağlayacaktır.

Gelecekte çalışanların bilgi güvenliği önlemlerine dair tutumlarının yanında niyet ve davranışlarının da incelenmesi, araştırmanın farklı örneklem grupları üzerinde gerçekleştirilmesi, araştırma modelinde yer alan değişkenler arasındaki aracı ve düzenleyici ilişkilerin incelenmesi konuya farklı bakış açıları kazandırabilir.

## Kaynakça

Ajzen, I., & Fishbein, M. (1975). A Bayesian Analysis of Attribution Processes. Psychological Bulletin, 82(2), 261-277.

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. In Action Control (s. 11-39). Springer, Berlin, Heidelberg.

Albers, S. (2010). PLS and Success Factor Studies in Marketing. V. E. Vinzi, W. W. Chin, J. Henseler, & H. Wang (Eds.), Handbook of Partial Least Squares Concepts, Methods and Applications. Almanya: Springer.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security Policy Compliance: User

Acceptance Perspective. 45th Hawaii International Conference on System Sciences (s.3317-3326). IEEE.

Anderson, J. B. (2021). Inadequacy of Risk Acceptance Criteria for Cloud Services Adoption: A Qualitative Generic Study. (Yayımlanmamış doktora tezi), Capella University School of Business, Minnesota.

Antoniou, G. S. (2015). Design an Effective Information Security Policy for Exceptional Situations in an Organization: An Experimental Study. Nova Southeastern University, Graduate School of Computer and Information Sciences.

Arshinskiy, L. & Shurkhoetsky, G. (2022). Methods of Information Security in Cloud Storages. Transportation Research Procedia, 61(2022), 455-461.

Boone, R. G. (2011). Factors Impacting Innovation Acceptance in Product Development Organization: Utilizing Technology Acceptance Model. (Yayımlanmamış doktora tezi), Capella University School of Business and Technology, Minnesota.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523-548.

Chen, V. V. (2012). Ensuring the Effectiveness of Information Security Policy: The Development and Validationof an Information Security Model. State University of New York College of Computing and Information, New York.

Cherdantseva, Y., & Hilton, J. (2013). A Reference Model of Information Assurance & Security. IEEE Proceedings of ARES 2013, (s.1-11). Resenburg.

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A.(2022). Overview of Social Engineering Attacks on Social Networks. Procedia Computer Science, 198(2022), 656-661.

Chin, W. W. (1998). Issues and Opinion on Structural Equation Modeling. MIS Quarterly, 22(1), vii-xvi.

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity Awareness in the Context of the Industrial Internet of Things: A Systematic Literature Review. Computers in Industry, 137(2022), 1-16.

Çatuk, C. (2018). Siber Risklerin Karşısında KOBİ'lerin Bilgi Güvenliği Farkındalıklarını Ölçen Bir Ölçek Geliştirme: Gaziantep Örneklemi. (Yayımlanmamış doktora tezi), Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü, Gaziantep.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319-340.

Davis, F. D. (1993). User Acceptance of Information Technology: System Characteristics, User Perception and Behavioral Impacts. Int. J. Man-Machine Studies, 38, 475-487.

Dhillon, G., & Backhouse, J. (2000). Technical Opinion: Information System Security Management in the New Millennium. Communications of the ACM, 43(7), 125-128.

Eminağaoğlu, M., & Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11(4), 1-5.

Erkan, A. (2006). Bilgi Güvenliği Yönetim Sistemi İçin Otomatik Bir Araç. (Yayımlanmamış yüksek lisans tezi), Orta Doğu Teknik Üniversitesi Enformatik Enstitüsü, Ankara.

Ersoy, E. V. (2012). ISO/IEC 27001 Bilgi Güvenliği Standardı. Ankara: ODTÜ Yayıncılık.

Farrel, A. M. (2010). Insufficient Discriminant Validity: A Comment on Bove, Pervan, Beatty, and Shiu (2009). Journal of Business Research, 63(3), 324-327.

Feistel, G. (2014). Technology Acceptance Model: Factor Influencing Consumers' Intent to Use Electronic Personal Health Records. (Yayımlanmamış doktora tezi), Central Michigan University School of Health Sciences, Michigan.

Fornell, C., & Larcker, D. F. (1981). Structural Equation Models with Unobservable Variables

and Measurement Error: Algebra and Statistics. Journal of Marketing Research, 18(3), 382-388.

Gabbard, R. B. (2004). Applying the Technology Acceptance Model to Online Education. (Yayımlanmamış doktora tezi), Trident University International Faculty of the College of Business Administration, California.

Garson, G. D. (2016). Partial Least Squares: Regression and Structural Equation Models. Asheboro, NC: Statistical Associates Publishers.

Gelişken, U. (2009). 10 Adımda Bilgisayar Güvenliği. İstanbul: KODLAB Yayıncılık.

Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. Procedia Computer Science, 181, 59-66.

Güldüren, C. (2015). Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi. (Yayımlanmamış doktora tezi), Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Hair, J. F., Hult, T. M., Ringle, C., & Sarstedt, M. (2014a). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). America: SAGE Publications.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). Indeed a Silver Bullet. Journal of Marketing Theory and Practice, 1(2), 139-151.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to Use and How to Report the Results of PLS-SEM. European Business Review, 31(1), 2-4.

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014b). Partial Least Squares Structural Equation Modeling (PLS-SEM) An Emerging Tool in Business Research. European Business Review, 26(2), 106-121.

Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W., …Calantone, R. J. (2014). Common Beliefs and Reality About PLS: Comments on Rönkkö and Evermann (2013). Organizational Research Methods, 17(2), 182-209.

Henseler, J. (2017). Partial Least Squares Path Modeling Advanced Methods for Modeling Markets. International Series in Quantitative Marketing. Retrieved on 10 10, 2021 from file:///C:/Users/nurg%C3%BCl/Downloads/Henseler2017-PLSPathModeling.pdf

Henseler, J., Hubona, G., & Ray, P. A. (2015). Using PLS Path Modeling in New Technology Research: Updated Guidelines. Industrial Management & Data Systems, 116(1), 2-20.

Hernandez, T. E. (2021). Strategies for Implementing Internet of Things Devices in Manufacturing Environments. (Yayımlanmamış doktora tezi), Walden University Information Systems and Technology, Minnesota.

Hu, L. T., & Bentler, P. M. (1999). Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives. Structural Equation Modeling: A Multidisciplinary Journal, 6(1), 1-55.

Hulland, J. (1999). Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies. Strategic Management Journal, 20, 195-204.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security Awareness: The First Step in Information Security Compliance Behavior. Journal of Computer Information Systems. Retrieved on 03 11, 2020 from https://doi.org/10.1080/08874417.2019.1650676

İleri, Y. Y. (2018). Kurumsal Bilgi Kaynaklarına Erişimde Güvenlik: Hekimlerin Şifre Yönetimine Yönelik Bir Araştırma. Uluslararası Sağlık Yönetimi ve Stratejileri Araştırma Dergisi, 4(1), 15-25.

Jones, C. M. (2009). Utilizing the Technology Acceptance Model to Assess Employee Adoption of Information Systems Security Measures. (Yayımlanmamış doktora tezi), Nova Southeastern University School of Business and Entrepreneurship, Florida.

Jouini, M., Rabai, L. B., & Aissa, A. B. (2014). Classification of Security Threats in Information Systems. 5th International Conference on Ambient Systems, Networks and Technologies,

(s. 489-496). Belgium.

Karaoğlan Yılmaz, F. G., Yılmaz, R., & Sezer, B. (2014). Üniversite Öğrencilerinin Güvenli Bilgi ve İletişim Teknolojisi Kullanım Davranışları ve Bilgi Güvenliği Eğitimine Genel Bir Bakış. Bartın Üniversitesi Eğitim Fakültesi Dergisi, 3(1), 176-199.

Kim, J. A. (2005). User Acceptance of Web-Based Subscription Databases: Extending the Technology Acceptance Model. (Yayımlanmamış doktora tezi), The Florida State University College of Information, Tallahassee.

Koohang, A., Sargent, C. S., Nord, J. H., & Paliszkiewicz, J. (2022). Internet of Things (IoT): From Awareness to Continued Use. International Journal of Information Management, 62 (2022), 1-10.

Koza, M. (2008). Bilgi Yönetimi: Bilgiyi Doğru Kullanmak. İstanbul: Kum Saati Yayınları.

Laudon, K. C., & Laudon, J. P. (2011). Management Information Systems Managing The Digital Firm. England: Pearson Education Limited.

Lee, V. C. (2015). Examining the Relationship between Autonomy, Competence, and Relatedness and Security Policy Compliant Behavior. (Yayımlanmamış doktora tezi), Northcentral University Graduate Faculty of the School of Business and Technology Management, Arizona.

Lionel, B. (2020). Examining the Relationship Between Cybersecurity-Employee Vulnerabilities and Reduction of Security Breaches in Information Technology Organization. (Yayımlanmamış doktora tezi), Colorado Technical University Computer Science, Colorado.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. MIS Quarterly, 16(2), 173-186.

Marakas, G. M., & O'Brien, J. A. (2013). Introduction to Information Systems. USA: The McGraw-Hill Companies.

Matney, J. L. (2022). Exploring the Cybersecurity Challenges of Quantum -Resistant Solution Implementations for Securing Internet of Things Data.(Yayımlanmamış doktora tezi), Colorado Technical University, Colorado.

McCumber, J. R. (1990). Information Systems Security: A Comprehensive Model. 14th National Computer Security Conference. Washington, s.334

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual Differences and Information Security Awareness. Computers in Human Behavior, 69, 151-156.

Merhi, M. I. (2014). Creating An Information Systems Security Culture Through An Integrated Model of Employees Compliance. (Yayımlanmamış doktora tezi), the Graduate School of the University of Texas-Pan American, Edinburg.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. Procedia-Social and Behavioral Sciences, 147, 424-428.

Mitnick, K. D., & Simon, W. L. (2005). Aldatma Sanatı. (N. E. Tezcan, Çev.) Ankara: ODTÜ Yayıncılık.

Ngufor, F. A. (2020). Understanding the Perspective of Information Security Managers on Insider Threat: A Phenomenology Investigation. (Yayımlanmamış doktora tezi), Northcentral University School of Business, Arizona.

Nitzl, C. (2016). The Use of Partial Least Squares Structural Equation Modelling (PLS-SEM) in Management Accounting Research: Directions for Future Theory Development. Journal of Accounting Literature, 37, 19-35.

Özer, G., Özcan, M., & Aktaş, S. (2010). Muhasebecilerin Bilgi Teknolojisi Kullanımının Teknoloji Kabul Modeli (TKM) İncelenmesi. Journal of Yasar University, 3278-3293.

Parsons, K., Calic, D., & Pattinson, M. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. Computer & Security, 66, 40-51.

Peltier, T. R. (2001). Information Security Risk Analysis. Auerbach. Retrieved on 30 12, 2021 from https://books.google.com.tr/books?id=O0_fO2Xvp98C&printsec=frontcover&dq=information+security+definition&hl=tr&sa=X&redir_esc=y#v=onepage&q=information%20security&f=false

Raggad, B. G. (2010). Information Security Management: Concepts and Practice. Boca Raton: CRC Press. Retrieved on 30 12, 2021 from https://books.google.com.tr/books?id=PQ3SBQAAQBAJ&pg=PA537&dq=ISO/IEC+27002+(2005)+information+security&hl=tr&sa=X&ved=2ahUKEwjZ2LHf6MD0AhXBSvEDHVBWB7QQ6wF6BAgFEAE#v=onepage&q=ISO%2FIEC%2027002%20(2005)%20information%20security&f=false

Rome, J. D. (2021). Understanding Adoption Barriers of Superior Technologies to Authenticate and Protect Users from Ongoing Cyber Threats. (Yayımlanmamış doktora tezi). Ashford University, Arizona.

Safa, N. S., Sookhak, M., Solms, R. V., Furnell, S., Ghani, N. AN., & Herawan, T. (2015). Information Security Conscious Care Behaviour Formation in Organizations. Computers & Security, 53, 65-78.

Solms, B. v. (2000). Information Security-The Third Wave? Computer & Security, 19(7), 615-620.

Solms, B. v. (2006). Information Security-The Fourth Wave. Computer & Security, 25(3), 165-168.

Solms, B. v. (2010). The 5Waves of Information Security-From Kristian Beckman to Present. IFIP International Information Security Conference, SEC: 2010 Security and Privacy – Silver Linings in the Cloud, (s. 1-8).

Şahinaslan, E. (2010). Standartlara Dayalı Bilgi Güvenliği Risk Analiz ve Ölçümleme Metodolojisinin Bankacılık Sektörüne Özgü Modellenmesi ve Uygulama Yazılımının Geliştirilmesi. (Yayımlanmamış doktora tezi), Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Teo, T., & Lee, C. B. (2008). Understanding pre-service teachers' computer attitudes: Applying and Extending the Technology acceptance model. Journal of Computer Assisted Learning, 24(2), 128-143.

Tientcheu, P. P. (2021). Security Awareness Strategies Used in the Prevention of Cybercrimes by Cybercriminals. (Yayımlanmamış doktora tezi), Walden University College of Management and Technology, Minnesota.

Turan, M. (2019). Ceza Almadan Tedbir Al Kişisel Veriler Bilgi Güvenliği İlkeleri İle Nasıl Korunur? KVKK İşletmenizin Kanuna Uyumlu Olması için Ne Yapmalısınız? İstanbul: Cinius Yayınları.

Vargas Moya, E. (2021). Security and Privacy Risks Associated of Cloud Computing: A Correlational Study. (Yayımlanmamış doktora tezi), Capella University School of Business and Technology, Minnesota.

Wright, C. (2008). The IT Regulatory and Standards Compliance Handbook: How to Survive an Information Systems Audit and Assessments. Burlington: Syngress Publishing

Young, R. (2010). Evaluating the Perceived Impact of Collaborative Exchange and Formalization on Information Security. Journal of International Technology and Information Management, 19(3), 2.

Yurtsever, G. (2013). Bilgi Güvenliği İçin Ne Yapmalı? Turcomoney Dergisi. Retrieved on 12 10, 2020 from https://www.turcomoney.com/bilgi-guvenligi-icin-ne-yapmali.html