

**T.C.
SAKARYA ÜNİVERSİTESİ
İŞLETME ENSTİTÜSÜ**

**BİLİŞİM TEKNOLOJİSİ ÇALIŞANLARININ SİBER
HİJYEN DAVRANIŞ NİYETİNİ ETKİLEYEN
FAKTÖRLERİN BELİRLENMESİ: BİR MODEL
ÖNERİSİ VE AMPİRİK TEST**

DOKTORA TEZİ

**Tuğçe KARAYEL
ORCID: 0000-0002-5556-225X**

Enstitü Anabilim Dalı : Yönetim Bilişim Sistemleri

**Tez Danışmanı: Doç. Dr. Adem AKBIYIK
ORCID: 0000-0001-7634-4545**

TEMMUZ – 2024

Tuğçe KARAYEL tarafından hazırlanan “Biliřim Teknolojisi alıřanlarının Siber Hijyen Davranıř Niyetini Etkileyen Faktörlerin Belirlenmesi: Bir Model Önerisi Ve Ampirik Test” bařlıklı bu tez, 27/05/2024 tarihinde Sakarya Üniversitesi Lisansüstü Eđitim ve Öğretim Yönetmeliđi'nin ilgili maddeleri uyarınca yapılan Tez Savunma Sınavı sonucunda bařarılı bulunarak, jürimiz tarafından Doktora Tezi olarak kabul edilmiřtir.

Danıřman: Do. Dr. Adem AKBIYIK

Sakarya Üniversitesi

Jüri Üyeleri: Prof. Dr. Nihal SÜTÜTEMİZ

Sakarya Üniversitesi

Dr. Öğr. Üyesi Alpaslan KİBAR

Sakarya Üniversitesi

Do. Dr. Osman USLU

Afyon Kocatepe Üniversitesi

Do. Dr. Metin SAYGILI

Sakarya Uygulamalı Bilimler Üniversitesi

 SAKARYA ÜNİVERSİTESİ	T.C. SAKARYA ÜNİVERSİTESİ İŞLETME ENSTİTÜSÜ TEZ SAVUNULABİLİRLİK VE ORJİNALLİK BEYAN FORMU	Sayfa: 1/1
Öğrencinin		
Adı Soyadı	:	Tuğçe KARAYEL
Öğrenci Numarası	:	D199054001
Enstitü Anabilim Dalı	:	Yönetim Bilişim Sistemleri
Enstitü Bilim Dalı	:	
Programı	:	Doktora
Tezin Başlığı	:	Bilişim Teknolojisi Çalışanlarının Siber Hijyen Davranış Niyetini Etkileyen Faktörlerin Belirlenmesi: Bir Model Önerisi ve Ampirik Test
Benzerlik Oranı	:	% 9
Sakarya Üniversitesi İşletme Enstitüsü Lisansüstü Tez Çalışması Benzerlik Raporu Uygulama Esaslarını inceledim. Enstitünüz tarafından Uygulama Esasları çerçevesinde alınan Benzerlik Raporuna göre yukarıda bilgileri verilen tez çalışmasının benzerlik oranının herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi beyan ederim.		
		10 / 05 / 2024 Tuğçe KARAYEL
Sakarya Üniversitesi İşletme Enstitüsü Lisansüstü Tez Çalışması Benzerlik Raporu Uygulama Esaslarını inceledim. Enstitünüz tarafından Uygulama Esasları çerçevesinde alınan Benzerlik Raporuna göre yukarıda bilgileri verilen öğrenciye ait tez çalışması ile ilgili gerekli düzenleme tarafımda yapılmış olup, yeniden değerlendirilmek üzere gsbtez@sakarya.edu.tr adresine yüklenmiştir. Bilgilerinize arz ederim.		
		10 / 05 / 2024 Doç. Dr. Adem AKBIYIK
Uygundur		
Danışman Unvanı / Adı-Soyadı:	Doç. Dr. Adem AKBIYIK	
Tarih:	10/ 05 / 2024	
İmza:		
☐ Kabul Edilmiştir ☐ Reddedilmiştir	Enstitü Birim Sorumlusu Onayı	
EYK Tarih ve No: / / 20.... /		

ÖNSÖZ

Akademik hayatımın ilk başlangıcından doktora sürecinin bitimine kadar beni yönlendiren, destekleyen ve vizyonunu paylaşan kıymetli hocam, danışmanım Doç. Dr. Adem AKBIYIK'a ne kadar teşekkür etsem azdır. Tez yolculuğunda, konumun ortaya çıkması ve son halini almasına kadar ilgisini hiç eksik etmediği için minnettarım.

Doktora derslerini hayranlıkla dinlediğim ders anlatımı, bilgisi ve uzmanlığı ile akademik çalışmalarına yön veren Prof. Dr. Nihal SÜTÜTEMİZ'e tez sürecinin her aşamasında verdiği emek ve katkılarından dolayı teşekkürü bir borç bilirim. Tez savunma jürisinde yer alan ve fikirleri ile katkı sunan, Doç. Dr. Osman USLU, Doç Dr. Metin SAYGILI ve Dr. Öğr. Üyesi Alpaslan KİBAR'a teşekkür ediyorum.

Bu tez çalışmasını yürütürken, değerli rehberlikleriyle bana yol gösteren Prof. Dr. Necdet SAĞLAM ve Prof. Dr. Semran SAĞLAM'a teşekkürü borç bilirim.

Dr. Öğr. Üyesi Tuğba KOÇ, Arş. Gör. Bahadır AKTAŞ, Arş. Gör. Ecenur DEMİR, Arş. Gör. Seren ÖZSOY ve Arş. Gör. Oğuzhan ARI'ya tez sürecimde vermiş oldukları fikir ve katkıları için teşekkür ederim.

Özel bir teşekkür Dr. Esengül ÖZDEMİR ALTINIŞIK'a tez sürecinde beni motive ettiği ve güzel temennileri ile bana hep destek olduğu için minnettarım.

Hayatım boyunca desteklerini bir an olsun bile esirgemeyen ve bu günlere gelebilmemde birçok fedakarlık yapan canım aileme şükran borçluyum.

Hayat arkadaşım, sevgili eşim Bekir KARAYEL'e yoğun iş temposuna rağmen bana olan ilgisini bir an bile eksiltmediği için minnettarım. Tez sürecimde beni her konuda motive eden ve desteğini hiçbir zaman bırakmayan kıymetli eşime ne kadar teşekkür etsem azdır.

Tuğçe KARAYEL

27.05.2024

İÇİNDEKİLER

KISALTMALAR	iii
TABLolar	v
ŞEKİLLER	vi
ÖZET.....	vii
ABSTRACT	viii

GİRİŞ	1
-------------	---

BÖLÜM 1. KAVRAMSAL ÇERÇEVE.....	9
---------------------------------	---

1.1. Siber Güvenlik ile İlgili Kavramlar	9
1.1.1. Siber	10
1.1.2. Siberetik	10
1.1.3. Siber Uzay	12
1.1.4. Siber Güvenlik	13
1.2. Siber Güvenliğin Hedefleri.....	17
1.3. Siber Güvenliğin Fonksiyonları	19
1.4. Siber Güvenliğin Bileşenleri	21
1.4.1. Süreç.....	22
1.4.2. Teknoloji	22
1.4.3. İnsan	23
1.5. Siber Saldırıları.....	23
1.5.1. Zararlı Yazılımlar.....	24
1.5.2. Virüsler.....	26
1.5.3. Solucanlar.....	29
1.5.4. Truva Atları.....	30
1.5.5. Hizmet Engelleme (DOS/DDOS) Saldırıları	30
1.5.6. Sosyal Mühendislik.....	33
1.5.7. Oltalama – Yemleme (Phishing) Saldırıları.....	34
1.5.8. İstenmeyen E-posta (Spam)	37
1.5.9. SQL Enjeksiyon Saldırısı.....	39
1.6. Siber Güvenlik Kültürü	41
1.7. Bilgi Güvenliği	42

BÖLÜM 2. TEORİK ALTYAPI.....	43
------------------------------	----

2.1. Siber Güvenlik Davranışına Yönelik Teoriler.....	43
2.1.1. Koruma Motivasyon Teorisi	45
2.1.2. Teknoloji Tehditlerinden Kaçınma Teorisi.....	47
2.1.3. Genel Caydırıcılık Teorisi.....	50
2.2. Siber Güvenlikte Koruma Motivasyon Teorisi	53
BÖLÜM 3. ARAŞTIRMA YÖNTEMİ	61
3.1. Araştırma Problemi	61
3.2. Araştırma Tasarımı.....	63
3.3. Araştırma Modeli ve Hipotezleri.....	65
3.4. Anakütle ve Örneklem.....	71
3.5. Enstrümanın Geliştirilmesi ve Veri Toplama Yöntemi.....	73
3.6. Yapısal Eşitlik Modellemesi.....	75
BÖLÜM 4. ANALİZ VE BULGULAR.....	78
4.1. Demografik İstatistikler.....	78
4.2. Güvenilirlik Analizi.....	81
4.3. Açıklayıcı Faktör Analizi	84
4.4. Modele Ait Analizler.....	88
4.5. Araştırma Modeli ve Hipotez Testleri.....	96
4.6. Uzaktan ve Hibrit Çalışanların Hipotez Testleri	101
4.7. Bulguların Kuramsal Temel Çerçevesinde Değerlendirilmesi.....	108
SONUÇ VE ÖNERİLER.....	113
KAYNAKÇA	121
EKLER.....	146
ÖZGEÇMİŞ.....	155

KISALTMALAR

AFA	: Açıklayıcı Faktör Analizi
AH	: Kullanıcı Bilgileri ve Şifre Hijyeni
AVE	: Ortalama Açıklanan Varyans
BDT	: Bilişsel Değerlendirme Teorisi
BG	: Bilgi Güvenliği
BGF	: Bilgi Güvenliği Farkındalığı
BGUE	: Birleştirilmiş Güvenlik Uygulamaları Enstrümanı
BS	: Bilgi Sistemleri
BSGP	: Bilgi Sistemleri Güvenlik Politikası
BT	: Bilgi Teknolojileri
CB-SEM	: Kovaryans Temelli YEM
CHBI	: Siber Hijyen Davranışsal Niyet
DDOS	: Dağıtılmış Hizmet Reddi
DFA	: Doğrulayıcı Faktör Analizi
DOS	: Hizmet Reddi
EP	: E-posta Hijyeni
GCT	: Genel Caydırıcılık Teorisi
HBT	: Alışkanlıklar
IOT	: Nesnelerin İnterneti
ISO	: Uluslararası Standardizasyon Örgütü
ISP	: Bilgi Güvenliği Politikasına Tutum
KMO	: Kaiser-Meyer-Olkin
KMT	: Koruma Motivasyon Teorisi
MET	: Mantıklı Eylem Teorisi
PDT	: Planlı Davranış Teorisi
PLS-SEM	: Kısmi En Küçük Kareler Yem
PS	: Algılanan Önem
PV	: Algılanan Güvenlik Açığı
RC	: Yanıt Maliyeti
RE	: Yanıt Yeterliliği
SE	: Öz Yeterlilik
SG	: Siber Güvenlik
SH	: Saklama Alanı ve Cihaz Hijyeni

SM	: Sosyal Medya Hijyeni
SN	: Öznel Normlar
SQL	: Structured Query Language
SPSS	: Statistical Package for the Social Sciences
TH	: Veri Aktarım Hijyeni
TTKT	: Teknoloji Tehditlerinden Kaçınma Teorisi
UTB	: Uluslararası Telekomünikasyon Birliği
VIF	: Varyans Artış Değerleri
YEM	: Yapısal Eşitlik Modellemesi



TABLÖLAR

Tablo 1: Literatür İncelemesi	57
Tablo 2: Modeldeki Faktörlerin Kaynakları	74
Tablo 3: PLS-SEM vs CB-SEM Karşılaştırması	76
Tablo 4: Tüm Katılımcıların Demografik Özellikleri	78
Tablo 5: Uzaktan Çalışan Katılımcıların Demografik Özellikleri	79
Tablo 6: Hibrit Şeklinde Çalışan Katılımcıların Demografik Özellikleri	80
Tablo 7: Ölçek İfadelerinin İç Tutarlılık Analizi Sonuçları	82
Tablo 8: Örneklem Büyüklüğü İçin KMO Katsayıları.....	85
Tablo 9: KMO Test Sonuçları.....	85
Tablo 10: Faktör Yükleri.....	86
Tablo 11: Formatif Maddelerin Dış VIF Değerleri.....	89
Tablo 12: Reflektif Değişkenlerin Inner- VIF Değerleri	90
Tablo 13: Formatif Yapının Dış Yükleri Ve Ağırlıkları	90
Tablo 14: Ölçüm Modeli Sonuçları.....	91
Tablo 15: Ayrışma Geçerliği Sonuçları (Fornell Larcker Kriteri)	93
Tablo 16: Ayrışma Geçerliliği Sonuçları (HTMT Kriteri).....	94
Tablo 17: Çapraz Yükler Kriterinin Sonuçları.....	95
Tablo 18: R^2 Değerlendirmesi	98
Tablo 19: Model R^2 Değeri	98
Tablo 20: Yol Analizi Sonuçları	98
Tablo 21: Uyum İndeksleri	100
Tablo 22: Uzaktan Çalışanların Yol Analizi Sonuçları.....	103
Tablo 23: Hibrit Şeklinde Çalışanların Yol Analizi Sonuçları	105
Tablo 24: Uzaktan ve Hibrit Çalışanların Karşılaştırılmalı Gösterimi	107

ŞEKİLLER

Şekil 1: Siber Güvenlik Olaylarındaki İnsan Hatası Oranı.....	2
Şekil 2: Zararlı Yazılımlardan Etkilenen Organizasyonların Oranı	3
Şekil 3: En Çok Kullanılan Siber Saldırı Yöntemleri.....	4
Şekil 4: Sibernetik Özellikleri	11
Şekil 5: Siber Güvenliğin Alt Dalları	15
Şekil 6: Siber Güvenliğin Hedefleri	18
Şekil 7: Siber Güvenliğin Fonksiyonları	20
Şekil 8: Siber Güvenliğin Bileşenleri	22
Şekil 9: Siber Saldırı Türleri.....	25
Şekil 10: Zararlı Yazılımların Oranı.....	25
Şekil 11: Hizmet Reddi Saldırılarının Sınıflandırılması.....	31
Şekil 12: Oltalama Saldırıları	37
Şekil 13: Siber Güvenlik, Bilgisayar Güvenliği ve Bilgi Güvenliği Trendleri.....	44
Şekil 14: Teknoloji Tehditlerinden Kaçınma Teorisi Modeli	49
Şekil 15: Genel Caydırıcılık Teorisi	51
Şekil 16: Temel Araştırma Yaklaşımları	64
Şekil 17: Araştırma Modeli	71
Şekil 18: Araştırma Modeli Smart-PLS Çıktısı	97

ÖZET

Karayel, T (2024). *Bilişim teknolojisi çalışanlarının siber hijyen davranış niyetini etkileyen faktörlerin belirlenmesi: bir model önerisi ve ampirik test* (Yayımlanmamış doktora tezi). Sakarya Üniversitesi.

Organizasyonlar kritik öneme sahip dijital varlıklarını, iş performansına ve kurum itibarına ciddi zararlar veren siber saldırılardan korumak zorundadır. Siber saldırıların amacı zaman içinde değişmemiştir ancak yapay zekâ tekniklerinin kullanımının artmasıyla saldırı yöntemlerinde ciddi bir değişim yaşanmaktadır. Siber saldırılardan korunma teknolojik yöntemlere yatırım yaparak olduğu gibi aynı zamanda insan sermayesine yatırım yaparak da olabilmektedir. İnsan odaklı önlemler alınmadan sadece teknik/teknolojik önlemler siber saldırılarla baş etmede yetersiz kalacaktır. Çünkü herhangi bir sistem ağının güvenliğinde en zayıf halka insan unsurudur. Organizasyonların en önemli insan unsuru ise çalışanlarıdır. Çalışanlar kasıtlı olarak veya ihmal yoluyla bilgi güvenliği açısından büyük bir tehdit oluşturmaktadır. Çalışanların zayıf bilgi güvenliği davranışları bu alandaki ana sorundur. BT çalışanları ise diğer çalışanlardan farklı olarak kurumun hassas bilgilerine erişme yetkileri vardır. Bununla birlikte uzaktan çalışanların işyeri ağından uzak olması nedeniyle siber saldırganlar için daha cazip bir kitledir. Günümüzde hem ekonomik hem konfor açısından avantajlı yeni çalışma düzenleri olan uzaktan ve hibrit çalışma birçok kurumda uygulanmaktadır. Özellikle BT çalışanlarının işlerinin uzaktan veya hibrit şeklinde çalışmaya yatkın olması sebebiyle hem kurumlar hem çalışanlar açısından sıklıkla tercih edilmektedir. Bu nedenle bu tez çalışması uzaktan veya hibrit şeklinde çalışan BT çalışanlarına odaklanmaktadır. Araştırma kapsamında, BT çalışanlarının siber hijyen davranışsal niyetini etkileyen faktörler koruma motivasyon teorisi, mantıklı eylem teorisi ve alışkanlıklar teorisi ekseninde incelenmektedir. LinkedIn platformu üzerinden toplanan 535 BT çalışanı katılımcı verisi SPSS 22.0 ve Smart-PLS 4.0 istatistiksel paket programları ile analiz edilmiştir. Araştırma sonuçlarına göre, algılanan güvenlik açığı haricinde KMT' nin tüm öğelerinin siber hijyen davranışını önemli ölçüde belirlediğini göstermektedir. Öznel normlar faktörünün uzaktan ve hibrit şeklinde çalışan BT uzmanlarının siber hijyenini etkilemediği bulunmuştur. Uzaktan çalışan BT uzmanlarının bilgi güvenliği politikalarına tutumunun siber hijyeni etkilemediği, hibrit şeklinde çalışan BT uzmanlarının bilgi güvenliği politikalarına tutumunun siber hijyeni etkilediği bulunmuştur. Güvenlik alışkanlıklarının ise uzaktan çalışanların siber hijyeni önemli derecede etkilediği, hibrit şeklinde çalışanların siber hijyenini etkilemediği bulunmuştur. Uzaktan ve hibrit şeklinde çalışma sisteminin gitgide daha yaygın hale geleceğinden araştırma sonuçları tüm kurumlar için önem arz etmektedir. Ayrıca, araştırma sonuçlarının, politika yapıcılara ve yöneticilere kurumsal güvenlik politikalarına uyumu kolaylaştırmak için uzaktan veya hibrit şeklinde çalışan BT uzmanlarının siber hijyenini iyileştirmeye yönelik öneriler sunarak bir rehber olacağı düşünülmektedir.

Anahtar Kelimeler: Siber Güvenlik, Bilgi Güvenliği, Siber Hijyen, Koruma Motivasyon Teorisi, Bilgi Güvenliği Politikası

ABSTRACT

Karayel, T. (2024). *Identification of factors influencing the cyber hygiene behavioral intentions of information technology employees: a model proposal and empirical testing*. (Unpublished doctoral thesis). Sakarya University.

Organizations must protect their digitally critical assets from cyber attacks, which can cause serious damage to business performance and corporate reputation. The purpose of cyber attacks has not changed over time, but with the increasing use of artificial intelligence techniques, there is a serious change in attack methods. Protection against cyber attacks occurs not only through investment in technological methods but also through investment in human capital. Without taking human-focused measures, relying solely on technical/technological measures will be insufficient in dealing with cyber attacks. This is because the weakest link in any system network is the human element. The most important human element within organizations is their employees. Employees pose a major threat to information security, either intentionally or through negligence. Poor information security behavior of employees is the main problem in this field. IT employees, unlike other employees, have the authority to access sensitive information of the institution. Remote workers are a better target for cyber attackers because they are away from the workplace network. Nowadays, remote and hybrid working, which are new working patterns that are advantageous both in terms of economy and comfort, are implemented in many institutions. It is frequently preferred by both institutions and employees, especially since IT employees tend to work remotely or hybridly. Therefore, this thesis study focuses on IT employees who work remotely and hybridly. Within the scope of the research, the factors affecting the cyber hygiene behavioral intention of IT employees are examined in the combination of protection motivation theory, rational action theory and habits theory. The data of 535 IT professionals collected via the LinkedIn platform were analyzed using the statistical software packages SPSS 22.0 and Smart-PLS 4.0. According to the research findings, aside from perceived security vulnerability, all elements of KMT significantly determine cyber hygiene behavior. The factor of subjective norms was found to have no effect on the cyber hygiene of both remote and hybrid-working IT professionals. It was found that the attitude of remote-working IT professionals towards information security policies did not affect cyber hygiene. However, it was found that the attitude of hybrid-working IT professionals towards information security policies did affect cyber hygiene. It was found that security habits significantly influenced the cyber hygiene of remote workers. However, it was found that security habits did not affect the cyber hygiene of hybrid workers. Research results are important for all institutions, as remote and hybrid working systems will become increasingly common. In addition, it is thought that the research results will serve as a guide for policy makers and managers by providing recommendations to improve the cyber hygiene of IT professionals working remotely and hybridly to facilitate compliance with corporate security policies.

Keywords: Cyber Security, Information Security, Cyber Hygiene, Protection Motivation Theory, Information Security Policy

GİRİŞ

“Savunmasız bir dijital ekosistem ve küresel bir dijital salgının eşiğindeyiz.”

Siber Güvenlik Uzmanı Chris Krebs

(McMillan, 2021)

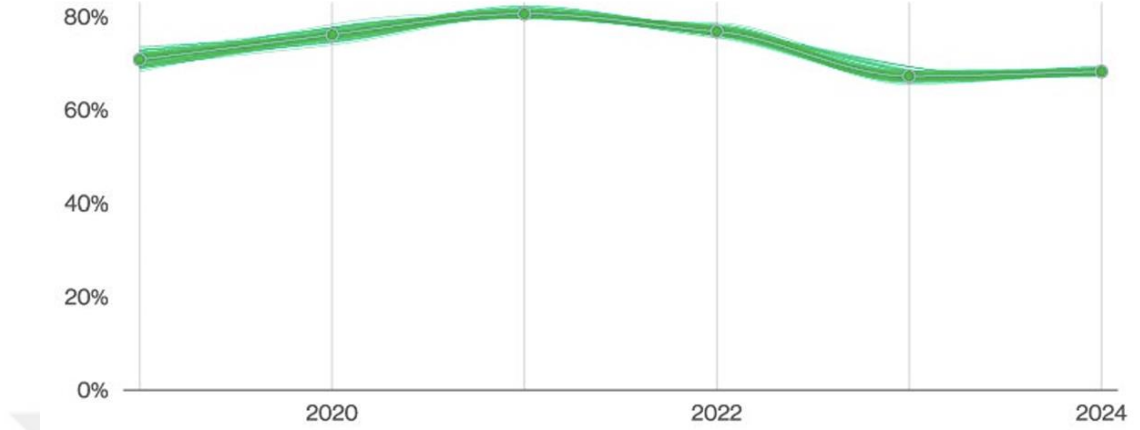
İçinde bulunduğumuz dijital çağda internet, elektriğe benzer şekilde, birçok kurumun onsuz çalışamayacağı temel bir meta olarak kabul edilmektedir. İnternet kurumlar için bu kadar önemli bir meta iken aynı zamanda siber güvenlik ihlalleri açısından sorunlara neden olan büyük bir ağıdır. Kurumlar önemli dijital varlıklarını siber saldırılara karşı korumak için teknolojik önlemlere büyük miktarda harcama yapmaktadır (Safa vd., 2019).

Kamu ve özel sektör kurumları çoğunlukla teknik çözümlere odaklandığından dijital varlıklarını güvence altına almakta başarısızlık yaşamaktadır. Siber güvenliğinin multidisipliner bir konu olması ve insan faktörünün önemli bir rol oynaması nedeniyle sadece teknolojik alanlarına odaklanmak yetersiz kalmaktadır. İnsan faktörleri, kurumsal bilgi güvenliği olaylarının önemli bir bölümünden sorumludur (Kalhoru vd., 2021). Bu alanda kullanıcı davranışları önemli bir güvenlik faktörü olarak karşımıza çıkmaktadır. Siber güvenlikte insan faktörü doğrudan veya dolaylı olarak güvenlik olaylarının büyük bir kısmını oluşturarak birçok kurumsal bilgi güvenliği ihlaline neden olur (Al-Shanfari vd., 2022).

IBM tarafından hazırlanan bir raporda bilgi güvenliği olaylarının %95'inin insan hatasından kaynaklandığı tespit edilmiştir (Howarth, 2014). Enisa'ya göre ise, veri ihlallerinin yaklaşık %77'si insan zafiyetinden kaynaklanmaktadır (Enisa, 2022). Verizon (2024) 94 ülkenin siber güvenlik olayını incelemiş ve olayların %68'inin insan hatasından kaynaklı olduğu tespit edilmiştir (*Şekil 1*).

Şekil 1

Siber Güvenlik Olaylarındaki İnsan Hatası Oranı



Kaynak:(Verizon Business, 2024)

Siber saldırganlar bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini kendi çıkarları doğrultusunda değiştirmek için yapay zekâ gibi farklı yöntemler kullanırken, kullanıcılar ise kasıtlı olarak veya ihmal yoluyla bilgi güvenliği açısından büyük bir tehdit oluşturmaktadır. Hesap bilgilerini paylaşmak, internetten herhangi bir yazılım indirmek, şifreleri yapışkan kâğıda yazmak, kimlik numaralarını kullanıcı adı veya şifre olarak kullanmak yaptıkları hatalara örneklerdir. Kullanıcıların ihmali, bilgisizliği, bilinçsizliği, ilgisizliği ve dirençleri genellikle güvenlik ihlallerinin nedenleridir. Kullanıcıların zayıf bilgi güvenliği davranışları bu alandaki temel sorundur (Safa vd., 2015, 2016). Bu noktada çalışanlara bilgi güvenliği farkındalığı kazandırmak ve zayıf bilgi güvenliği davranışlarını önlemek kurumlar adına önemlidir (Al-Shanfari vd., 2022). Literatürde özellikle kurumlar için önemli bir insan kaynağı olan BT çalışanlarının zayıf bilgi güvenliği davranışının nasıl iyileştirilebileceği ve bilgi güvenliği farkındalığını etkileyen faktörler hakkında sınırlı sayıda çalışma vardır (Safa vd., 2015, 2016). Bu araştırma kapsamında sunulan model kullanıcıların bu alandaki davranış riskini azaltmaya çalışmayı amaçlamaktadır.

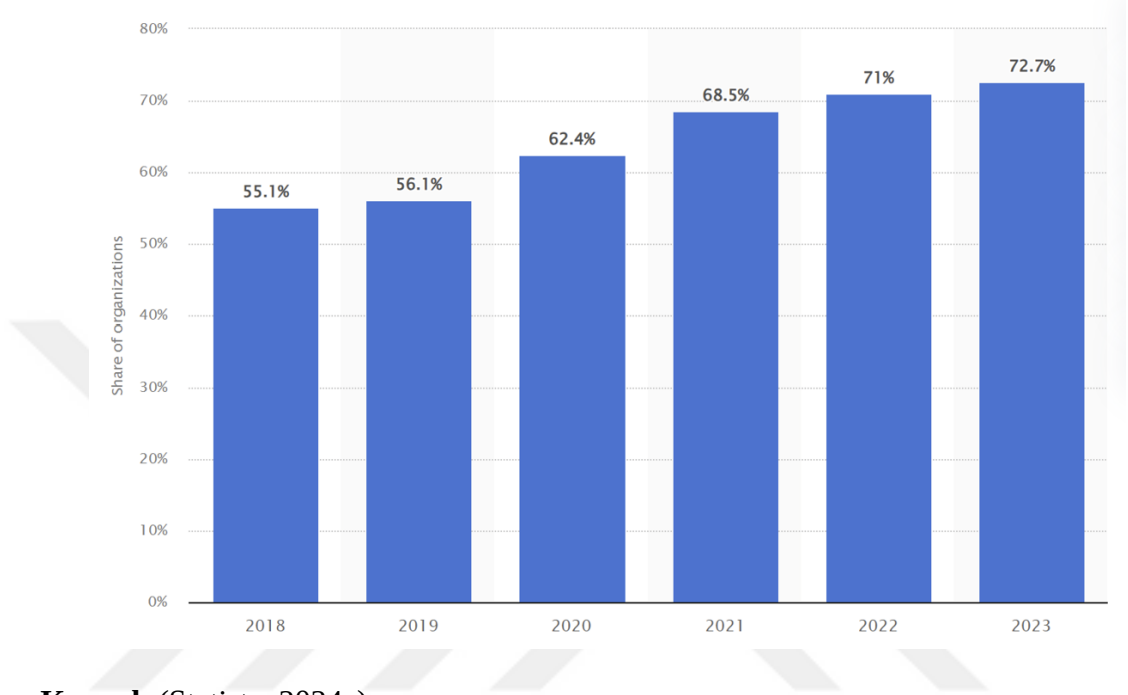
Araştırmanın Önemi

Küresel ölçekte tüm sektörler ve her büyüklükteki organizasyon siber risk altındadır. Siber saldırıların sıklığı, hacmi ve karmaşıklığı her yıl artarak kurumlara ek maliyetlere neden olmaktadır. Dünya genelinde siber suç maliyetlerinin 2025 yılına kadar 10,5 trilyon dolar olacağı ön görülmektedir (Ene, 2023). Statista (2024) tarafından hazırlanan raporda siber

saldırılardan etkilenen organizasyonların oranı 2023 yılı itibari ile %72 olmuştur (Şekil 2).

Şekil 2

Zararlı Yazılımlardan Etkilenen Organizasyonların Oranı



Kaynak:(Statista, 2024a)

Kurumlar için siber tehditler iç tehdit ve dış tehdit olmak üzere iki gruba ayrılmaktadır. Dış tehditler zararlı yazılımlar, fidye yazılımları ve siber saldırganlardan oluşturmaktadır. İç tehditler ise çalışanlar, paydaşlar ve ortaklardan oluşmaktadır. En önemli iç tehdit ise çalışanlardır (Joshi vd., 2012) ve genellikle bir kurumun en önemli ve yıkıcı güvenlik açığı, kendi çalışanlarıdır (Howarth, 2014). Britanya'da yapılan bir araştırmada, Birleşik Krallık merkezli kurumlardaki bilgi güvenliği olaylarının %58' inin içeriden gelen tehditlerden kaynaklandığı ortaya çıkmıştır. Bunların %33'ü çalışanların kurumun bilgi güvenliği yönergelerine veya politikalarına uymamasından kaynaklandığı bulunmuştur (Pwc, 2017). Intel'in güvenlik uzmanlarıyla yaptığı bir anket çalışmasında, veri ihlallerinin %43'ünün kurum çalışanlarının davranışlarından kaynaklandığı ortaya çıkmıştır (Rajab ve Eydgahi, 2019). Kurum çalışanları açısından başka bir örnek olay ise şu şekilde gelişmiştir; Airbus firması, Türk Hava Yolları şirketinde çalışan bir personelin bilgisayarına virüslü bir program indirmesi nedeniyle siber saldırıya uğramış ve güvenlik ihlali yaşamıştır (Pandagle, 2023a).

Cisco (2014) tarafından gerçekleştirilen araştırmaya göre ise, çalışanların %44'ü iş cihazlarını denetim olmadan başkalarıyla paylaştığı, %46'sı evden çalışırken iş ve kişisel bilgisayarları arasında dosya aktarımı yaptığı ve %25'i şifrelerini iş arkadaşlarıyla paylaştığı bulunmuştur.

Verizon (2024) siber güvenlik olaylarının yaklaşık %40' ı kimlik bilgilerinin ele geçirilmesi üzerinden, yaklaşık %20' sinin ortalama teknikleri kullanılarak ve yaklaşık %20'sinin bilgi sistemlerindeki güvenlik açıklarından kaynakladığını ortaya çıkarmıştır (Şekil 3).

Şekil 3

En Çok Kullanılan Siber Saldırı Yöntemleri



Kaynak: (Verizon Business, 2024)

Kurumlar, veri toplama, analiz etme ve kullanma konusunda beceri sahibi olan ayrıca erişim sahibi oldukları kullanıcıların verilerini korumaktan sorumlu olan BT uzmanlarının eylemlerine her geçen gün daha fazla bağımlı hale gelmektedir (Albrechtsen ve Hovden, 2009; Herath ve Rao, 2009b; Posey vd., 2015). Savaş vd. (2015), bilgi güvenliğindeki sorunların temel nedeninin BT uzmanlarının güvenlik zincirindeki en savunmasız halka olmasından kaynaklandığı belirtmektedir. Ayrıca kurumlar için vazgeçilmez bir çalışan grubunu olduğu gibi aynı zamanda tehdit faktörü de olabilmektedir. Örneğin Çin'deki ünlü bir şirkette çalışan bir BT uzmanı yaklaşık 155.000 kurum bilgisini farklı bir kuruma satmıştır (Ma, 2022). Bu eylem, kurum için

mali kayıp, itibar kaybı ve kişisel gizlilik ihlali suçlamaları da dahil olmak üzere ciddi sonuçlara neden olmuştur (Stanton vd., 2015). Dolayısıyla BT çalışanları kurumlar için önemli bir güvenlik kaynağı iken aynı zamanda iç tehdit ve potansiyel tehditlerinde kaynağı olabilmektedir.

Çalışanlar üzerinden yapılan bir araştırmada bilgi güvenliği ihlallerinin yarısından fazlasının personelin bilgi güvenliği politikalarına yetersiz uyumundan kaynaklandığı tespit edilmiştir (Humaidi ve Balakrishnan, 2015). Kurumlar bilgi güvenliği ve araçlarının teknolojik yönüne yatırım yapsa da, çalışanlara gereken ilginin gösterilmemesi nedeniyle güvenlik olaylarının ve ihlallerinin sayısı önemli bir sorun olmaya devam edecektir (Ifinedo, 2012).

Kurumların çalışanlarının dünyanın her yerinden çalışmasına izin verdiği uzaktan ve hibrit çalışma sisteminde siber güvenlik daha da önemli hale gelmiştir. Uzaktan çalışanlar, kurum işlerini kurumsal güvenlik koruması olmayan ağlar (ev ağı-kişisel ağ) üzerinden yaptıklarından dolayı siber saldırganların sıklıkla hedefinde olmaktadır. Uzaktan çalışmanın veri ihlallerine artışa neden olan önemli bir faktör olduğu tespit edilmiştir (IBM, 2021).

Araştırmalar, kurumların çalışan davranışındaki iyileştirmeler yoluyla güvenlik ihlallerinin riskini % 45-70 oranında azaltabileceğini göstermiştir (Aberdeen Group, 2015). Kurumların çalışanlarına siber güvenlik üzerine eğitim, öğretim ve farkındalık programlarını uygulamadan önce çalışanlarını neyin motive ettiğini ve hangi faktörlerin güvenlik davranışı gerçekleştirmede etkili olduğunu araştırması ve belirlemesi gerekmektedir. Bu faktörler belirlendikten sonra çalışanlara uygun eğitimler ve farkındalık programları sunulmalıdır. Siber güvenlik eğitim ve öğretim programları sayesinde çalışanlar, potansiyel güvenlik riskleri ve tehditlerinin farkında olmaları için gerekli yetkinlikleri ve becerileri kazanacaktır. Bu araştırmanın çalışanların bilgi ve bilgisayar güvenliği davranışı kısaca siber hijyen davranışını anlamada kurumlara yol gösterici olacağı düşünülmektedir.

Araştırmanın Amacı ve Problemi

Bu çalışmada geliştirilen model, çalışanların güvenlik tehditleri ve bu tehditlerle başa çıkma eylemlerine ilişkin siber hijyen davranışsal niyetlerini etkileyen faktörleri açıklamaktadır. Bu doğrultuda araştırma kapsamında ele alınacak temel araştırma problemi “Koruma motivasyon teorisi faktörleri, mantıklı eylem teorisi faktörleri ve

alışkanlıklar teorisi faktörleri bilişim sektöründe uzaktan veya hibrit çalışanların siber hijyen davranışlarını nasıl etkiler?” olarak belirlenmiştir. Bu temel araştırma problemini cevaplamak adına aşağıdaki alt sorulara cevap aranacaktır.

- 1) Koruma motivasyon teorisi faktörleri BT çalışanlarının siber hijyenini nasıl etkiler?
- 2) BT çalışanlarının güvenlik alışkanlıkları siber hijyeni nasıl etkilemektedir?
- 3) Çalışma tipine (uzaktan ve hibrit) göre BT çalışanlarının siber hijyenini etkileyen faktörler nasıl farklılık gösterir?

Temel araştırma problemi ve alt araştırma problemler dahilinde bu çalışmada, bilişim sektöründe uzaktan veya hibrit şekilde çalışanların siber hijyenini etkileyen faktörler üzerine güvenilir ve geçerli bir model geliştirilmek istenmektedir.

Araştırma Metodolojisi

Araştırmanın amacı doğrultusunda, nicel araştırma yönteminin kullanılması uygun görülmüştür. Literatürde tanımlayıcı olarak ifade edilen nicel araştırma yönteminin seçilmesinde araştırmanın amacı, araştırma problemleri ve çalışmanın hedef ana kütlesi kriterleri etkili olmuştur. Araştırma modelinin test edilmesi için gerekli verilerin toplanması aşamasında veri toplama yöntemi olarak birincil veri toplama kaynaklarından olan anket yöntemi tercih edilmiştir. Uzaktan çalışanlarının bulunmasının ve birebir görüşmenin zor olacağı nedeniyle veriler **LinkedIn** platformu üzerinden toplanmıştır. **LinkedIn** platformu üzerinden Türkiye’de yaşayan, bilişim sektöründe uzaktan veya hibrit şeklinde çalışan 18 yaş ve üzeri bireylere çevrimiçi anket uygulanmıştır. Veri toplama işlemi 15.08.2023-15.11.2023 tarihleri arasında, gönüllü katılımcılardan gerçekleştirilmiştir. Veri toplama için Sakarya Üniversitesi Etik Komisyonundan gerekli etik kurul onayı alınmış olup ilgili karar Ek-2’de sunulmuştur.

Araştırmanın verilerinin toplanması, tesadüfi olmayan örnekleme tekniklerinden amaçlı örnekleme tekniği kullanılarak yapılmıştır. Çalışma evreninin daraltılması adına çalışmanın kaynakları ve imkanların dahilinde örneklemin seçileceği sektör sadece bilişim sektörü olarak belirlenmiştir. Bilişim sektörü uzaktan ve hibrit şeklinde çalışmaya diğer sektörlerle kıyasla daha yatkın olması nedeniyle seçilmiştir. Ayrıca dijital okuryazarlık derecesinin daha yüksek olması, organizasyon içinde kritik görevlerde bulunması ve bilgi kaynaklarına erişim yetkilerinin sınırsız olması sebebiyle de seçilmiştir. Kritik görevlerde bulunan ve işletme bilgilerine tam erişimi olan çalışanların

siber hijyeni diğer sektör çalışanlara kıyasla daha önemlidir. Çünkü bu çalışanlar BT varlıklarına ve değerli bilgilere en fazla erişime sahip olan çalışanlardır ve bu nedenle siber saldırganların en değerli hedefi olmaktadır (Greengard, 2016; Torton vd., 2018).

Araştırma problemlerinden hareketle ve araştırmanın amacına uygun olarak öncelikle tanımlayıcı analiz, güvenilirlik analizi, açıklayıcı faktör analizi, doğrulayıcı faktör analizi ve son olarak yol analizi gerçekleştirilmiştir. Araştırma modelini test etmek amacıyla çok değişkenli istatistik analiz yöntemlerinden olan Yapısal Eşitlik Modellemesi kullanılmıştır. Söz konusu tüm analizlerin gerçekleştirilmesinde ise SPSS 22.0 ve Smart-PLS 4.0 programlarından faydalanılmıştır.

Araştırmanın Katkıları ve Sınırlılıkları

Bu araştırma, bireysel davranışın kritik bir rol oynadığı uzaktan ve hibrit çalışma gibi yeni ortaya çıkan çalışma tarzlarına önemli teorik ve pratik katkılar sunmaktadır. İlk olarak, uzaktan ve hibrit çalışan BT uzmanlarının siber hijyenini inceleyen çalışma olarak literatüre katkı sağlamaktadır. İkinci olarak, siber hijyen davranışları rasyonel eylemler olduğundan, çalışma siber hijyen davranışsal niyetleri koruma motivasyon teorisi, mantıklı eylem teorisi ve alışkanlıklar teorisinin kapsamında inceleyerek güvenilir ve geçerli bir model geliştirmiştir. Pratikte ise bu çalışma, uzaktan ve hibrit şeklinde çalışan BT uzmanlarının siber güvenlik farkındalığını artırmayı amaçlayan politika yapıcılara değerli bir rehberlik sağlayacaktır. Son olarak, yöneticilere bireysel davranışları kurumsal güvenlik politikalarıyla uyumlu hale getirme konusunda yardımcı olacaktır.

Her araştırmada olduğu gibi bu araştırmanında kapsam, metodoloji, içerik ve örneklem konusunda bazı kısıtları bulunmaktadır. Öncelikle, ilk kısıt araştırma sektör olarak sadece BT çalışanlarına odaklanmış olmasıdır. BT çalışanlarına yapılan bu araştırmada, sektör noktasında kısıtlama yapılmıştır. Araştırmanın bir diğer kısıtı ise çalışma sonucunda elde edilen bulgular, örnekleme göre değişiklik gösterebileceğinden, mevcut çalışma sonunda yapılan değerlendirmeler verilerin toplandığı örneklem ile sınırlı olduğudur.

Bilgi güvenliği alanında araştırma yapmak ve veri toplamak kurumları tehlikeye atabileceğinden kurumlardan bilgi almak oldukça zor olmaktadır. Ancak araştırma bulgularının genelleştirilmesi adına daha büyük bir örneklem grubu ve daha fazla sektör ile araştırma modelinin test edilmesi gelecek araştırmalara önerilmektedir. Ayrıca örneklem grubuna farklı ülkelerin çalışanlarının katılarak ülkeler arası karşılaştırılma yapılması önerilmektedir. Sonuç olarak, organizasyonlarda siber güvenlik olaylarının

nasıl önlenebileceği konusunda çalışanların siber hijyen davranışları ve siber güvenlik farkındalığı gibi insan faktörlerine odaklanılarak daha derinlemesine araştırmalar yapılması gerekmektedir.

Bu tez çalışmasının birinci bölümünde, siber güvenliğe dair genel konuların yer aldığı kavramsal çerçeve sunulmaktadır. İkinci bölümde siber güvenlik davranışlarında sıklıkla kullanılan teoriler tanıtılmakta ve devamında ilgili literatürün kapsamlı bir şekilde ortaya koyulması adına eleştirel kaynak incelemesine yer verilmektedir. Üçüncü bölümde ise, araştırmanın problemi, modeli ve hipotezleri ile araştırmanın evren ve örnekleme ve veri toplama yöntemleri ele alınmaktadır. Dördüncü bölümde, elde edilen verilerin analiz sonuçları ve bulgularına yer verilmektedir. Ayrıca bu bölümde, çalışmanın bulguları önceki çalışmalarla birlikte ele alınmış ve tartışılmıştır. Son olarak, sonuç ve öneriler kısmında ise, araştırma bulgularının teori ve uygulamaya yönelik katkılar tartışılmış, sınırlılıklar ve gelecekteki araştırmalara öneriler sunulmuştur.

BÖLÜM 1. KAVRAMSAL ÇERÇEVE

Bu bölümde araştırma ile ilgili kavramsal çerçeve yedi ana başlık üzerinden ele alınmaktadır. İlk olarak siber güvenlik ile ilgili temel kavramlar açıklanacaktır. Ardından, siber güvenliğin hedefleri, fonksiyonları ve bileşenleri açıklanacaktır. Devamında siber saldırı türleri tanıtılmaktadır. Son olarak ise siber güvenlik kültürü ve bilgi güvenliği kavramlarına değinilmiştir.

1.1. Siber Güvenlik ile İlgili Kavramlar

Bilgisayarların icadı ve ulaşılabilirliğinin artmasıyla başlayan insanlığın bilişim yolculuğu internetin kullanılmaya başlanması ve yaygınlaşması ile devam etmiş ve akabinde nesnelerin toplumla, daha sonrasında ise nesnelerin nesnelerle etkileşimi şeklinde ilerlemiştir.

Nesneler ile etkileşime geçtiği andan itibaren insanlık, siber ortamda güvenlik olgusunu ön planda tutmuştur. Maslow'un ihtiyaçlar hiyerarşisinde (Maslow, 1943) ikinci sırada yer alan güvenlik kavramı bilişim alanında da kendine yer edinmiştir. Bilişim teknolojilerinde yaşanan gelişmeler ve değişimler yıllara göre artan hızlarda farklılık gösterse de güvenlik olgusunu ve güvende olduğunu hissetme duygusunu sorgulatmayı her zaman başarmıştır. Bilgi teknolojilerinde yaşanan hızlı gelişmeler beraberinde güvenlik tehditlerini artırmıştır. Dijital ortamlarda verilerin ve bilgilerin güvenli olarak aktarılmasının aksine üçüncü şahıslar tarafından ele geçirilmesini kolaylaştırmıştır. Teknoloji hakkında yaptığı değerlendirmeleri ve geleceğe yönelik tahminleri ile tanınan yazar Alvin Toffler teknolojinin hızla geliştiğini fakat muhtemel tehditlerin teknolojinin büyüme hızından çok daha hızlı büyüdüğünü ifade etmektedir (Goodman, 2016). Bu doğrultuda, siber tehditler gün geçtikçe daha karmaşık hale gelmektedir (Symantec, 2020). Siber tehditlerin gitgide karmaşıklaşması, teknolojinin hızla büyüme göstermesiyle siber ortamın güvenliğinin sağlanmasını da zorlaştırmaktadır.

Teknolojik gelişmeler paralelinde tehdit ve tehlikelere karşı siber ortamın güvenliği önem kazanmıştır. Siber güvenliğin öneminin artması ve bu alan yazında yapılan çalışmaların sınırlı düzeyde olması alana olan yönelimleri arttırmıştır. Siber güvenliğe ilişkin tezler dikkate alındığında siber güvenlik başlığı altında ilk tez 2012 yılında yayımlanmıştır. 2012 yılından günümüze kadar toplam 86 tez çalışma yapılmıştır. Bu çalışmalar incelediğinde siber güvenlik kavramının multidisipliner yapıda olduğu görülmektedir.

Uluslararası ilişkiler, işletme gibi sosyal bilim alanlarındaki çalışmalarının yanı sıra bilgisayar mühendisliği, bilgisayar ve kontrol mühendisliği gibi fen bilim alanlarında da çalışmalar yapılmıştır.

Dijital sistemler yaklaşık 80 yıldır varlığını sürdürürken siber güvenlik yeni ve dinamik bir araştırma alanı olmuştur. İnternetin ilk ortaya çıktığı 1980'ler ve 1990'lara kadar siber güvenlik konularının tam ağırlığı gözlemlenememiştir. Bu zaman dilimlerinde, siber uzayın gelişimi ve karmaşıklığı katlanarak arttıkça siber güvenlik endişeleri de artmıştır. Siber güvenlik alanı halen siber uzayın hızlı büyümesine ve yeteneklerine yetişmeye çalışmaktadır(Edgar ve Manz, 2017, s. 33).

1.1.1. Siber

Siber güvenliği tanımlamadan önce siber olgusunun açıklanmasına ihtiyaç duyulmaktadır. Kelime kökü olarak yunanca “Kubernetes (yönetim, sevk, idare)” latince “subernetes(gemici, dümenci)” dayanan siber kelimesi güdüm bilimi şeklinde tanımlanan sibernetik kelimesinden gelmektedir (Nsugbe, 2021, s. 8).

Uluslararası Standardizasyon Örgütü (ISO 2012) siber kavramını “fiziksel şekilde var olmayan, teknolojik cihazlar ve kendisine bağlı ağlar aracılığıyla internet üzerindeki insan, yazılım ve hizmetlerin birbiri ile olan etkileşiminden oluşan karmaşık ortam” olarak tanımlamaktadır (Lehto ve Neittaanmaki, 2015).

Siber kelimesi askeri terminolojide bilgisayarlara ve bilgisayar ağlarında atıfta bulunulmak için kullanılmıştır (Turner, 2016, s. 7). Siber ve bilişim kavramları birbirinin yerine sıklıkla kullanılır fakat aslında iki kavram farklı anlamlara sahiptir. Siber kavramı elektronik sistemlerin ağ üzerinde bulunduğu ortam olarak tanımlanmaktadır. Bilişim ise bu ortam aracılığıyla bilginin üretilmesi anlamına gelmektedir. Sonuç olarak bilişim kavramı teknolojik kaynaklar kullanılarak üretilen bilgi veya ortaya çıkan sonuçların bütününe ifade etmektedir. Bilgisayar donanımı ve yazılımlar bilişim kavramının birer parçasını ifade etmektedir (Yalçın, 2019, s. 59).

1.1.2. Sibernetik

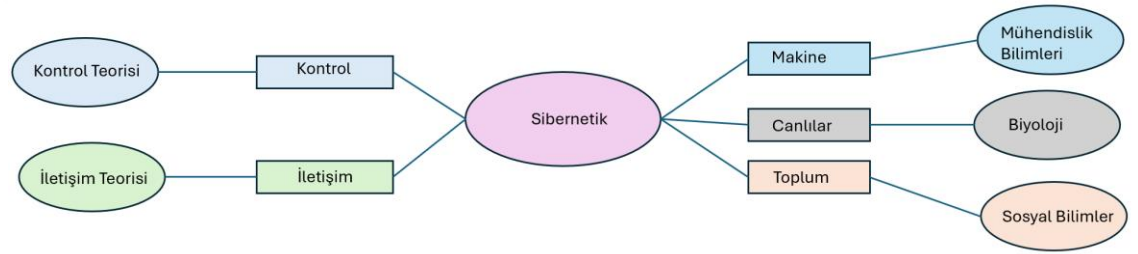
Sibernetik, canlı ve cansız fark etmeksizin tüm karmaşık sistemlerin yönetilmesini ve kontrol edilmesini inceleyen bilim dalıdır. Başka bir tanımla, bir makinenin veya insanın modern teknik kaynaklar çerçevesinde herhangi bir işi yönetmesini ve belli bir amaca ulaşmasını sağlayan bilimdir (*Türkçe Bilgi*, Erişim Tarihi:01.12.2021). Sezgin(2016)’e

göre sibernetik; insan-makine arasında etkileşim kuran, iletişim-kontrol süreçlerini içine alan, geri besleme için pratikler oluşturan mekanik sistem olarak tanımlanmaktadır. Kısaca sibernetik, makineler ile canlılar arasındaki ilişkilerin yönetilmesini ve denetimini araştıran bilim olarak tanımlayabiliriz (Şekil 4).

İçinde bulunduğumuz yüzyılda çok kapsamlı bir hal alan sibernetik kavramı birçok disiplinle ilişkili olarak tanımlanır olmuştur. Bu nedenle sibernetik, farklı alanları bir araya getiren multidisipliner bir alandır. Sibernetik özellikle insan ve teknolojiyi bir arayan getiren bilim dalı olarak tanımlanmaktadır(Novikov, 2016).

Şekil 4

Sibernetik Özellikleri



Kaynak: (Novikov, 2016).

Teknoloji kabul teorileri bireylerin bilişim teknolojileri tehditlerinden kaçınma davranışlarını tam olarak açıklayamadığından bu kaçınma veya korunma davranışlarını açıklamak için sibernetik teori geliştirilmiştir (Wiener, 1948). Sibernetik teori, beklenti teorisiyle uyumlu olduğu ve birey davranışlarını anlamak için geniş bir çerçeve sunmaktadır (Edwards 1992). Sibernetik süreçler her yerde mevcut olduğundan ve hemen hemen her kendi kendini düzenleyen sistemde tanımlanabilir olduğundan genel sistem teorisi olarak nitelendirilmektedir. Sibernetiğin ilkeleri sosyal psikoloji, sağlık psikolojisi ve örgütsel davranış teorilerinde geniş çapta uygulanmıştır (Carver ve Scheier, 1982).

Genellikle sibernetik olarak adlandırılan sibernetik teorisi, 20. yüzyılın ortalarında ortaya çıkan multidisipliner bir yaklaşımdır. Doğası gereği mekanik, biyolojik, sosyal veya mühendislikle ilgili olsun, bilgi akışını ve kontrol mekanizmalarını içeren sistemleri anlamak ve modellemekle ilgilidir.

Sibernetik teorisinin odak noktası, bireylerin davranışlarını geri bildirim döngüleri yoluyla kendi kendine düzenlemesidir. Bu sistem dört fonksiyondan oluşur; hedef, karşılaştırmacı, giriş ve çıkış (Carver ve Scheier 1982). Sibernetikte bir döngü, ortamdaki veya hedef

belirlemedeki rahatsızlık nedeniyle tetiklenir. Giriş fonksiyonu çevreyi algılar ve mevcut durumu hedef tarafından belirlenen bir referans değeriyle karşılaştıran karşılaştırmacıya sinyaller gönderir. Bir tutarsızlık tespit edilirse çıkış işlevi, tutarsızlığı ortadan kaldıracak veya azaltacak bir davranışı başlatır. Davranış çevre üzerinde bir etki yaratır, dolayısıyla mevcut durumu değiştirir ve bu da davranışın devam edip etmediğini belirlemek için referans değerle karşılaştırılır. Bu sürece negatif geri besleme döngüsü denir çünkü mevcut durum ile arzu edilen son durum arasındaki farklılığı azaltma işlevi görür (Liang ve Xue, 2009, s. 73).

Sibernetikte olumlu ve olumsuz geri bildirim döngüsü bulunmaktadır. Bireye yararlı olan BT'nin benimsenmesi olumsuz geri bildirim döngüsüyle açıklanırken, zararlı BT'den kaçınma olumlu geri bildirim döngüsüyle açıklanıyor. Benimseme istenen son duruma yaklaşmayı ve kaçınma ise istenmeyen son durumdan kaçınmayı içerdiğinden, bu olgular niteliksel olarak farklıdır (Liang ve Xue, 2009).

1.1.3. Siber Uzay

Toplumda bilginin daha hızlı bir şekilde yayılmasını sağlayan teknik cihazların ve araçların artmasıyla bilgi çağı ortaya çıkmıştır. İçinde bulunduğumuz bilgi çağında teknoloji, dokunduğu her alan için yeni terimler ve konular üretmiştir (Stehr, 2007). Bu terimlerden biri de siber uzaydır. Siber uzay terimi, ilk kez 1982 yılında William Gibson tarafından yazılan bir bilim kurgu romanında kullanılmıştır. İlerleyen zamanlarda ise bu terim popüler kültür tarafından benimsenmiş ve sıkça kullanılmaya başlanmıştır.

İngilizce 'de "cyberspace" olarak geçen Türkçe' de siber ortam, siber alan kelimeleri ile ifade edilen siber uzay kavramı birçok farklı tanımlara sahiptir. Siber uzay, bilgisayar ağlarından oluşan ve bu ağlar üzerinden iletişimin gerçekleştiği ortam olarak tanımlanmaktadır. Siber uzay, bilgi teknolojisi altyapısında kullanılan, cihazları, interneti verileri ve çeşitli ağları içeren küresel bir alandır. Siber uzay kısaca, iletişimin internet üzerinden gerçekleştiği elektronik ortam olarak da tanımlanabilir (Turner, 2016, s. 109). Uluslararası Telekomünikasyon Birliği (UTB) siber uzayı, internete, telekomünikasyona ve bilgisayar ağlarına doğrudan veya dolaylı olarak bağlı sistemler ve hizmetler olarak tanımlamaktadır. ABD'de 8 Ocak 2008 tarihinde siber güvenlik politikası imzalandı. Böylece siber uzayın ilk resmi tanımı yayınlanmış oldu. Bu politika da siber uzay, birbirine bağlı bilgi teknolojisi altyapıları ağı olarak tanımlanmıştır (Kramer vd., 2009).

Ulusal güvenlik strateji raporuna göre siber uzay, “doğrudan ve ya dolaylı olarak internete, e-haberleşme ve BT ağlarına bağlı olan tüm sistem ve hizmetler” olarak tanımlanmaktadır (Ulaştırma ve Altyapı Bakanlığı, 2020).

Kramer’e göre siber uzay, ağa bağlı bilgi sistemleri ve ilgili fiziksel altyapılar aracılığıyla bilgi oluşturmak, depolamak, güncellemek ve dağıtmak için kullanılan operasyonel bir alan olarak tanımlanmaktadır(Kramer vd., 2009). Sonuç olarak siber uzay internet, telekomünikasyon ağları, bilgisayar sistemleri ile birbirine bağlı bilgi teknolojisi altyapıları ağından oluşan amacı bilgi üretmek ve dağıtmak olan küresel bir alan olarak tanımlanabilir.

Doğası gereği tanımlanması zor bir kavram olan siber uzay, insan yapımı bir ekosistemdir. Kara, hava, deniz ve uzay alanları herhangi bir insan varlığı olmadan var olurken, siber uzay sürekli insan katılımını ve faaliyetlerini gerektirir. Tüm bilgi iletişim teknolojileri ağlarını, veri tabanlarını ve bilgi kaynaklarını küresel bir sanal sistemde birleştiren siber uzay ekonomiyi, siyaseti, güvenliği, psikolojiyi ve bilişimi içeren multidisipliner bir kavramdır (Grobler vd., 2011).

Siber uzayın kötü amaçlı kullanımı bir devlet için çeşitli güvenlik ihlallerine sebep olabileceğinden, siber uzay ulusal güvenliğin kritik bir bileşeni olarak vurgulanmaktadır. Siber uzayın ortaya çıkışı, gizlilik, bütünlük ve kullanılabilirlik ilkelerine ulaşmayı göreceli olarak zorlaştırmıştır. Çünkü internetin ilk çıkış sebebi her şeyi paylaşılabilir kılmak ve veri dağıtımını özgür kılmak olduğu için o dönemlerde güvenlik ön plana çıkmamıştır (Wamala, 2011).

Teknoloji ve bilgiyle dolu dünyamızda siber uzay, günümüz toplumunun ayrılmaz bir parçasıdır. Hem kişisel hem de profesyonel bağlamlarda, siber uzay, çoğu insanın günlük olarak gerçekleştirdiği faaliyetlerde oldukça etkili ve kolaylaştırıcı bir dijital araçtır (Klimburg, 2012; Soliman ve Siponen, 2022).

Yapılan tanımlar incelendiğinde siber uzay, halen büyümekte olan, kullancılarının her türlü veriye erişime imkan sağlayabilen yeni bir ortam olarak tanımlanabilmektedir. Siber uzay ile birlikte coğrafi mekan sınırları olmadan bireyler arasında bir bağlantı kurulmuştur.

1.1.4. Siber Güvenlik

Bilgisayarların icadından 21. yy başlangıcına kadar bilgisayar güvenliği ve bilgi güvenliği gibi terimler kullanılırken günümüzde bu kavramları temsilen şemsiye terim

olan “siber güvenlik” kullanılmaktadır. Güvenlik teriminin siber ortamda fiziksel güvenlikten yazılımsal güvenliğe olan yolculuğuna kısaca göz attığımızda ilk başlarda bilgisayarların fiziksel büyüklüklerinin devasa boyutta olması nedeniyle dış kapılardaki özel güvenlik personelleri ile korunmaktaydı. Güvenlik aşamaları, bilgisayarla çalışmaya yetkili insanların makinelere fiziksel erişimini sağlamak için tasarlanan özel izinler içeren süreçler içermektedir (Bayuk vd., 2012). Günümüzde ise bu özel izinlerin yerini çeşitli güvenlik yazımları almıştır.

BT güvenliği olarak da bilinen siber güvenliğin temel amacı, işletmenin bilgi teknolojileri altyapısını ve günlük operasyonları için gerekli bilgileri korumaktır. COVID-19 pandemisinin teknoloji kullanım ihtiyacını hızlandırmasıyla birlikte işletmeler, teknolojiyi kullanma ve benimseme baskısı altında kalmıştır (ABCNews, 2020). İşletmeler, iş yaparken önemli bilgilerini sistemler üzerinden aktardığı için herhangi bir siber tehdit nedeniyle verilerini, müşterilerini kaybedebilir ve bazı cezalara maruz kalabilmektedir. Küresel siber tehditler, her yıl artan veri ihlali ile hızlı şekilde büyümeye devam etmektedir. Güvenlik raporları, özellikle son yıllarda veri ihlalleri nedeniyle her yıl milyarlarca kişisel ve kurumsal verinin kötü niyetli saldırganlar tarafından ele geçirildiğini ortaya koymaktadır (Akdemir ve Tuncer, 2021, s. 398). Bu doğrultuda siber güvenlik yazılım ve donanım desteği işletmelerin bilgisini, bilgi işleme veya depolama sistemlerini korumada çözüm sağlamaktadır (Tam vd., 2021). Gartner’e göre, bilgi güvenliği ürün ve hizmetlerine dünya çapında yapılan harcamaların 2022’de yılında 170,4 milyar dolar olduğu tahmin edilmektedir (Morgan, 2019).

Siber güvenlik, sürekli değerlendirme ve yenilik gerektiren, hızla gelişen bir alandır. Siber güvenlik üzerine yeni terim ve kavramlar ortaya çıkmış ve literatürde bunlar hakkında birden çok farklı tanımlamalar yapılmıştır.

Kaspersky siber güvenliği, bilgisayarları, mobil cihazları, sunucuları, ağları, elektronik sistemleri ve verileri kısacası tüm BT varlıklarını kötü niyetli kişilerin siber saldırılarından koruma olarak tanımlanmaktadır (Kaspersky, 2019; Klimburg, 2012).

Ulusal güvenlik strateji raporuna göre siber güvenlik, “siber uzayı oluşturan bilişim sistemlerinin kötü amaçlı saldırılarından korunmasını, siber uzayda işlenen verinin-bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin güvence altına alınmasını, siber saldırıların ve olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri

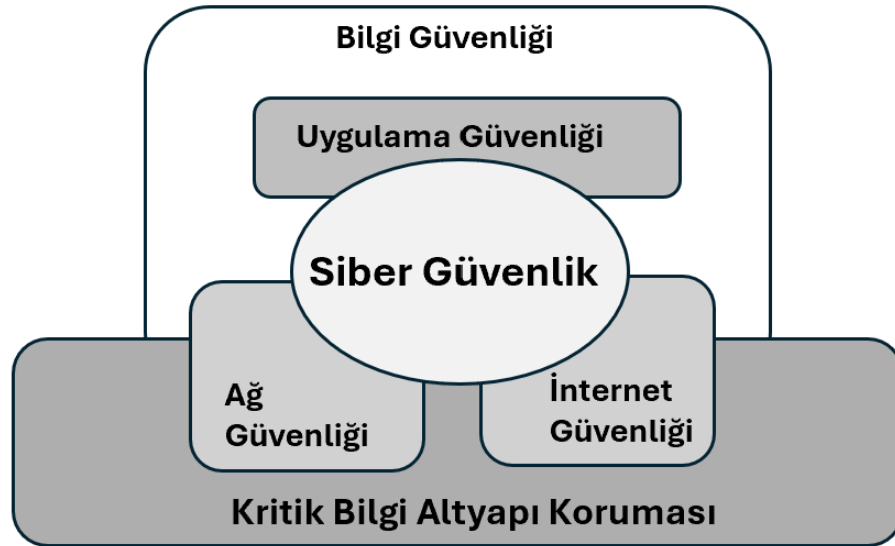
döndürülmesini kapsayan faaliyetler bütünü ” olarak tanımlanmaktadır (Ulaştırma ve Altyapı Bakanlığı, 2020).

UTB siber güvenliği şu şekilde tanımlamaktadır: “Siber güvenlik, siber ortamı, kurumu ve kullanıcının varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitimler, en iyi uygulamalar, güvence ve teknolojilerin toplamıdır. Kurumun ve kullanıcının varlıkları, ağa bağlı bilgi işlem cihazlarını, personeli, altyapıyı, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya depolanan bilgilerin toplamını içerir. Siber güvenlik, siber ortamdaki ilgili güvenlik risklerine karşı kurumun ve kullanıcı varlıklarının güvence altına alınmasını ve bu güvencenin sürdürülmesi için çaba göstermektedir” (ITU, 2008).

Siber güvenlik kavramı içinde bilgi güvenliği, ağ güvenliği, internet güvenliği ve uygulama güvenliği barındıran geniş kapsamlı bir terimdir(Klimburg, 2012; von Solms ve von Solms, 2018, s. 5).

Şekil 5

Siber Güvenliğin Alt Dalları



Kaynak: (Von Solms ve Von Solms, 2018, s. 5)

- Bilgi güvenliği: bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması ile ilgilidir.
- Ağ güvenliği: Ağlarda bilgi güvenliği amaçlarına ulaşmak için ağların tasarımı, geliştirilmesi ve işletilmesi ile ilgilidir.

- İnternet güvenliği: Kurumlarda ve evde internetle ilgili hizmetleri, BİT sistemlerini korumakla ilgilidir. İnternet güvenliği internet üzerinden gerçekleştirilen hizmetlerin kullanılabilirliğini ve güvenilirliğini de sağlar.

Siber güvenlik, sistemlerin ve verilerin dijital saldırılardan korunmasına atıfta bulunmak için kullanılan bir terimdir(Carlton ve Levy, 2017). Başka bir tanıma göre siber güvenlik, dijital kaynaklara ve verilere yetkisiz erişimi, kötüye kullanımı önlemek için alınan önlemler ve eylemler bütünüdür (Edgar ve Manz, 2017, s. 37).

Siber güvenlik kavramı ise genel olarak birkaç terimle birlikte açıklanır. Bunlar sırasıyla siber güvenliğin hedeflerini, bileşenlerini ve fonksiyonlarını yansıtır (Bayuk, 2009; Bayuk vd., 2012). Bunlar sırasıyla:

- Önlemek, tespit etmek, yanıtlamak(fonksiyonlar)
- İnsanlar, süreç, teknoloji(bileşenler)
- Gizlilik, bütünlük ve kullanılabilirlik(hedefler)

Bunlar ayrıca güvenlik uzmanlarının amaçlarını ve yöntemlerini açıklayan kavramlardır. Siber güvenliğin sadece güvenlik uzmanları veya güvenlik yazılımları tarafından sağlanamayacağını bu yüzden sadece teknoloji ile gerçekleştirilemeyeceği vurgulanmaktadır. Sistem veya organizasyonun güvenliği için kararları ve eylemleri ile güvenlik programlarının başarısında hayati bir rol oynayan diğer unsurda insandır. Ayrıca bireyler güvenli davranma motivasyonuna ve ilgisine sahip olsalar bile, önceden planlanmış bir süreç yoksa tehdidi önlemek, tespit etmek ve zarardan kurtulmak için nasıl hareket edeceklerini bireysel olarak bilemezler. Dolayısıyla güvenlik uzmanlarından güvenlik programlarını mevcut organizasyonel süreçlere dâhil etmeleri ve siber güvenlik hedeflerini gerçekleştirmek için teknolojiyi stratejik olarak kullanmaları beklenir(Bayuk vd., 2012).

Siber güvenlik hedefleri olarak gizlilik, bütünlük ve erişilebilirlik ilkeleri öne çıkmaktadır. Bu ilkelerden gizlilik, bir sistemin veya bilginin yayılmasını yetkili kullanımla sınırlandırma yeteneğini ifade eder. Bütünlük, kaydedilen ve rapor edilen bilgilerin özgünlüğünü, doğruluğunu ve kaynağını koruma yeteneğini ifade eder. Erişilebilirlik, bilginin yetkili kişiler tarafından kullanılabilir olmasını ifade eder (Bayuk vd., 2012). Bunlar aynı zamanda bilgi güvenliği hedefleri olarak da ele alınmaktadır. Bilgi güvenliği hedefleri, bilgisayarlar bulunmadan önce bilgiye uygulanıyordu. İnternet

teknolojilerinin ilk ortaya çıktığı zamanlarda erişilebilirlik ilkesi ön plana çıkarken gizlilik ve bütünlük ilkeleri geri planda kalmıştır. Bunun nedeni, internet ilk zamanlarda sadece kullanım amaçlı ve geliştirme amaçlı düşünülmüş olup gizlilik ve bütünlük ilkelerine önem verilmemiştir (Şenol, 2020). Fakat daha sonrasında hayatın her aşamasına yayılan bilgi teknolojileri, gizlilik ve bütünlük ilkelerini de ön plana çıkarmıştır.

Belirli bir sistemdeki her bilgi türü için gizliliğin, bütünlüğün ve erişilebilirliğin ne anlama geldiğini belirlemek siber güvenliğin öncelikli alanıdır. Özetle siber güvenlik, siber ortamda bilginin gizliliğine, bütünlüğüne ve erişilebilirliğine verilen zararı tespit etmek ve zararı önlemek için insanları, süreçleri ve teknolojiyi kullanma yöntemlerini ifade eder.

1.2. Siber Güvenliğin Hedefleri

Bilgisayarların ortaya çıktığı ilk zamanlarda bilgilerin korunmasına yönelik yalnızca birkaç geçerli yöntem vardı. Bunun başlıca nedeni bilgisayarların o zamanlarda pahalı olması sebebiyle az bulunması ve sıkı denetimler ile korunuyor olmasıydı. Önemli bilgileri içeren bilgisayar sistemleri, bilgiye erişimi olan ve programlama becerisine sahip sınırlı sayıda kişiler tarafından kullanılmaktaydı. Bu bilgilerin korunmasına yönelik ilk odak, bilgisayar sisteminin gerektiğinde tutarlı bir şekilde çalışabilmesini sağlamak için sistemin güvenilirliğini sağlamaktı. Sonuç olarak, bilgi koruması esas olarak bilgisayarlara fiziksel erişimi kısıtlama yoluyla başladı. Bilgisayar teknolojilerinin maliyeti azaldıkça kullanımı arttı bu doğrultuda odakta bilgisayarların güvenilirliği baskınken daha sonraları bilgisayarın korunmasından ziyade bilgisayar sistemlerinde tutulan bilgilerin korunması gerektiği önem kazanmaya başlamıştır. Bilgisayar donanımını ve yazılımını korumaktan bu sistemlerin içindeki bilgileri korumaya doğru bir kaymaya ve güvenlik zihniyetindeki değişime neden olmuştur. Ancak bu değişim, önce gizliliğe, ardından bütünlüğe ve ardından kullanılabilirliğe odaklanan yavaş bir evrimsel süreç olarak başlamıştır (Samonas ve Coss, 2014, s. 23).

Şekil 6

Siber Güvenliğin Hedefleri



Kaynak: Yazar tarafından oluşturulmuştur.

Güvenli bir bilgisayar sistemi, bilgilerin/verilerin gizliliğini korumalı, bütünlüğünü ve erişilebilirliğini sağlamalıdır. İzinsiz bir sızma yoluyla yetkisiz kişi/programlar, faaliyetlerin normal akışına zarar vermek amacıyla bir bilgisayara veya ağa girdiğinde bilgisayar sisteminin güvenliği tehlikeye girer (Ambalavanan ve Shanthi Bala S., 2019). Siber güvenlik, siber uzayı ve kullanıcıları yetkisiz erişim ve saldırılara karşı korumak için alınabilecek güvenlik önlemlerin bütünüdür. Bir siber savunma sisteminin temel hedefleri, verilerin gizli, bütünsel ve erişilebilir/kullanılabilir olmasını sağlamaktır.

Siber güvenlik, kişisel bilgileri, hükümet verilerini ve iş raporlarını yasa dışı sızma ve kötü amaçlı işlemlerden korumayı amaçlar. Ayrıca siber güvenlik, a) yazılım, araç ve ekipmanın korunmasını b) çeşitli tehdit ve saldırılara karşı korunan bilgilerin gizliliğinin, bütünlüğünün sağlanmasını ve garanti edilmesini kapsar(Fischer vd., 2005).

Gizlilik

Gizlilik, verilerin ve bilgilerin yetkisiz varlıklara veya kişilere kullanıma açık olması engelleyen özelliktir. Bir bilgisayar sisteminde gizlilik yeterince sağlanamazsa parola hırsızlığı ve istenmeyen e-postalar ile karşı kaşıya kalılabilmektedir. Gizlilik için genellikle uçtan uca şifreleme teknikleri kullanılmaktadır(Sinha vd., 2019, s. 1209).

Bütünlük

Veri-bilgi bütünlüğü, sistem yaşam döngüsü boyunca verilerin/bilgilerin doğruluğunun sağlanması ve sürdürülmesi anlamına gelmektedir. Bu durum verilerin/bilgilerin yetkisiz bir şekilde değiştirilmesini önlemektedir(Sinha vd., 2019, s. 1209). Bütünlük ilkesinin 3 hedefi vardır. Bunlar:

- a) Yetkisiz kullanıcıların veya programların verilerde/bilgilerde değişiklik yapmasını önlemek,
- b) Yetkili kullanıcıların uygunsuz veya yetkisiz değişiklikler yapmasını önlemek,
- c)Verilerin/bilgilerin ve programların iç ve dış tutarlılığını korumaktır (Merkow ve Breithaupt, 2014, s. 49).

Erişilebilirlik

Herhangi bir bilgi sisteminin amacına hizmet etmesi için, veri ve bilgilerin kullanılabilirliği son derece önemlidir. Bu, bilgileri işlemek ve depolamak için kullanılan bilgi işlem sistemlerinin, iletişim erişim kanalları ve güvenlik kontrollerinin düzgün çalışması anlamına gelir (Sinha vd., 2019, s. 1209). Erişilebilirlik ilkesi, özellikle acil durumlar veya felaketler sırasında verilerin/bilgilerin ve kaynakların erişilebilir durumda olmasına dayanmaktadır. Üç farklı nedenden dolayı erişilebilirlik ilkesi tehlikeye girmektedir. Bunlar:

- a) Kasıtlı saldırılar veya uygulamadaki fark edilmemiş kusurlar nedeniyle hizmet reddi,
- b) Doğal afetler (yangın, sel, fırtına veya deprem) veya insan eylemleri (bombalar veya grevler) gibi nedenlerle bilgi sistemi yetenek kaybı,
- c)Normal kullanım sırasında donanım arızalarıdır (Merkow ve Breithaupt, 2014, s. 49).

İnternet geniş bir ağıdır ve güvenlik ihlalleri için büyük bir potansiyele sahiptir. Siber saldırganlar, bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini ihlal etmek için çeşitli yöntemler kullanır bu sebeple kullanıcıların farkındalığı sık sık ölçülmelidir (Stanton vd., 2005).

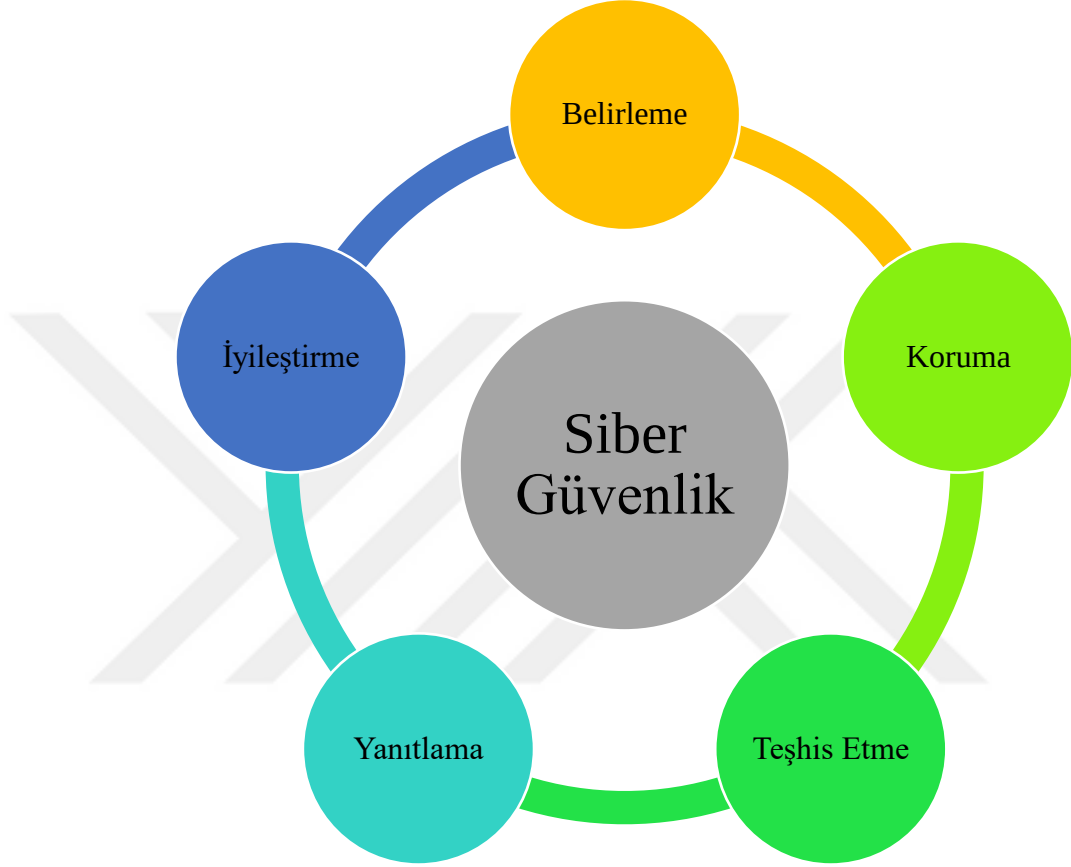
1.3. Siber Güvenliğin Fonksiyonları

Ulusal Standartlar ve Teknoloji Enstitüsü organizasyonların siber güvenlik risklerini azaltabilmesi ve daha iyi yönetilebilmesi için, siber güvenlik faaliyetlerinin sınıflandırılma ve değerlendirilme metodolojisini içeren Siber Güvenlik Çerçevesi

geliştirmiştir. Bu çerçeveye göre beş temel siber güvenlik fonksiyonu bulunmaktadır (Mahn, 2018)(Şekil 7).

Şekil 7

Siber Güvenliğin Fonksiyonları



Kaynak: Yazar tarafından oluşturulmuştur.

Belirleme

Kurum için siber güvenlik imajının oluşturulması varlıkların, sistemlerin, uygulamaların, verilerin, kurumsal bağlamın, operasyonel ihtiyaçların, sistemlere yönelik risklerin ve mevcut kaynakların belirlenmesiyle başlar. Bu aşama kurum neyi korumak istiyor ve ne ölçüde koruma sağlamak istiyorsa bunları belirlemelidir. Kurumun risk değerlendirmeleri nedir ve mevcut kaynakları nelerdir gibi sorulara cevap bulmasına yardımcı olur.

Koruma

Kurumların siber varlıklarını tehditlere karşı koruma sağlayacak koruma yeteneği geliştirmesi gerekir. Bu yetenek, olası siber güvenlik olaylarını önlemeye veya sınırlamaya ve söz konusu bu olayın gerçekleşmesi halinde olayı kontrol altına almaya

odaklanmalıdır. Koruma işlevinin amacı, kritik altyapı hizmetlerinin devamlılığını sağlamak için uygun korumaları geliştirmek ve uygulamaktır.

Tespit

Siber saldırı olayı önlemek için kurumun dijital varlıklarını zamanında izlemesi ve siber olay meydana gelmesi durumunda olası siber güvenlik ihlallerini tespit etme yeteneğini geliştirmesi gerekir.

Yanıtlama

Kurumlar, bir siber güvenlik olayı gerçekleştiğinde tepki verebilmek ve gerekli faaliyetleri uygulamak için bir yanıt verme mekanizması geliştirmek zorundadır. Bu faaliyetler, kurumun olayı analiz etmesine ve olası siber güvenlik olayının kurum üzerindeki etkisini azaltmasına olanak sağlayacaktır.

İyileştirme

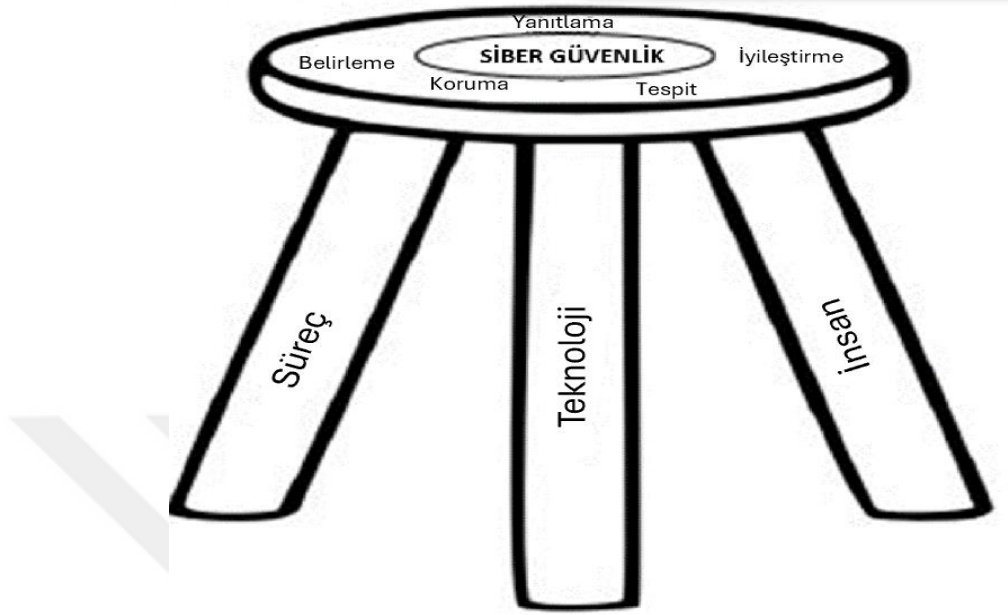
Kurumlar, bir siber güvenlik olayı nedeniyle etkilenen hizmetleri normal akışına geri döndürmek için planlar yapmalı ve gerekli eylemleri uygulamalıdır.

1.4. Siber Güvenliğin Bileşenleri

Teknoloji, insanlar ve süreçler ideal bir kurumsal siber güvenlik imajına ulaşmanın temel direkleridir. Organizasyonlar siber güvenlik fonksiyonlarını geliştirmek ve sürdürmek için teknolojinin, süreçlerin ve insanların ortak bir noktada birleşimini sağlamalıdır. Bu üç ana direk, üç ayaklı bir taburenin ayakları olarak gösterilebilir (*Şekil 8*). Şekilde görüldüğü gibi bu sütunlardan hiçbirisi göz ardı edilemez, kurum bir bileşende başarısız olursa siber güvenlikte de başarısız olacaktır (Büyükkılıç, 2018, s. 24–26).

Şekil 8

Siber Güvenliğin Bileşenleri



Kaynak: (Büyükkılıç, 2018, s. 24).

1.4.1. Süreç

Organizasyonların, kurum içinde hedeflenen siber güvenlik imajını elde etmesi için gerekli süreçleri geliştirmesi ve uygulaması gerekir. Bu süreçler, siber güvenlik fonksiyonlarını sağlamak için gerçekleştirilecek olan faaliyetleri açıklamaktadır. Özellikle farklı kişilerin aynı işlemleri her seferinde tam olarak aynı şekilde yapabilmelerini sağlamak için diğer bir deyişle belirli bir prosedürün tam olarak aynı şekilde yapılmasını sağlamak için prosedürler ayrıntılı talimatlar olarak açıklanmalıdır (Büyükkılıç, 2018).

1.4.2. Teknoloji

Güvenlik teknolojisi mevcut piyasada çok sayıda vardır ancak bunların işlevlerinin neler olduğunu ve siber altyapıda nereye uyduğunu tespit etmek gereklidir. İnternet teknolojileri ise, işletmelere ve müşterilerine birçok avantaj sağlamıştır ancak diğer taraftansa bilgi güvenliği ihlalleri ile karşı karşıya bırakmıştır. Siber uzayda güvenliği sağlamak için anti-virüs programları, güvenlik duvarı, kimlik doğrulama ve izinsiz giriş tespit sistemleri gibi teknolojik unsurlar kullanılmaktadır (Safa vd., 2015). Fakat kötü amaçlı kişiler, güvenlik ihlali oluşturmak için bilgisayarlar yerine insanları hedef

almaktadır (Furnell ve Clarke, 2012). Bu nedenle, siber uzay ortamında, güvenlik ihlalleri riskini azaltmak için çoklu güvenlik yaklaşımlarının(insan-teknoloji-süreç) uygulanması gereklidir.

1.4.3. İnsan

Bilgi teknolojileri veya bilgisayar güvenliğindeki odak noktalar çoğunlukla teknik sorunları oluşturmaktadır. Fakat güvenlik önlemleri konusunda güvenlik duvarları, anti virüs yazılımları gibi teknolojik araçların tek başına tam bir çözüm sağlayamayacağı bununla birlikte insani tarafların da ele alınmasının somut bir ihtiyaç olduğu giderek daha fazla kabul görmektedir. Gerekli teknolojilerin yanı sıra bütünsel bir güvenlik stratejisinin bir parçasını oluşturmak için insani yönlerin gerekliliği ön plana çıkmaktadır. İnsanlar güvenliği sağlamada kilit bir unsur temsil ederken, genellikle başarısızlık noktasıdır. Siber güvenlik, organizasyondan bireye toplumun tüm yönlerini etkilerken, sistemlerin tasarlanıp, güvenliğinin sağlanması için bireylere yol gösterici olacak politikaların geliştirilmesi gerekmektedir.

Davranış bilimi web sistemlerinin tasarımı, geliştirilmesi ve bakımı aşamalarında önemli bir rol oynamaktadır(Padayachee, 2012). Kullanıcılar, siber olaylara karşı bilinçlendirilmediğinde güvenlik faaliyetlerini bir engel olarak görebilmekte, güvenlik faaliyetlerinde zorluklar çıkarabilmekte ve güvenliği yanlış yorumlayabilmektedir(Cox, 2012). Kullanıcılar zorunlu bir şifre değişikliği ile karşı karşıya kaldıklarında tutumları ve davranışları değişir. Araştırmacılar, bu tür değişikliklerin kasıtlı olarak ertelendiğini ve gereksiz bir kesinti olarak kabul edildiğini ortaya çıkarmıştır(J. M. Stanton vd., 2005).

Güvenlik ihlallerinin yalnızca teknik çözümlerin uygulanmasıyla önlenemeyeceği yaygın olarak kabul edilmektedir. (Furnell vd., 2006; Parsons vd., 2014). Güvenlik sistemindeki en zayıf halka genellikle insan faktörüdür(Schneier, 2004). Son yıllarda, çalışanların şirketin bilgi güvenliğini nasıl etkileyebileceklerini araştıran çalışmalar yapılmıştır (McCormac vd., 2017; Shropshire vd., 2015). Örneğin, IBM Global Teknoloji Hizmetleri (2015) güvenlik ihlallerinin %95'ten fazlasının insan hatasının sonucu olduğunu ortaya çıkarmıştır(IBM, 2015, s. 7).

1.5. Siber Saldırıları

Siber saldırılar, küresel ölçekte her 39 saniyede bir meydana gelerek ciddi oranda artmaktadır (Washo, 2021) Yeni nesil saldırganlar her zamankinden daha güçlü ve

kullanımı kolay saldırı araçlarıyla dijital bir dünyada artmaya devam etmektedir. Bu nedenle siber saldırılara karşı mücadele etmek ve saldırıların hızına yetişebilmek her geçen gün daha da zorlaşmaktadır(Firdausi vd., 2010; Shaukat vd., 2020). Diğer bir yandan siber saldırılar, tüketicilerin güveninin yanı sıra bir şirketin statüsünü veya itibarının kaybetmesine neden olmaktadır(Sangani ve Vijayakumar, 2012).

Kötü amaçlı yazılım eğilimlerinin ve ağ güvenliği tehditlerinin detaylandırıldığı bir rapora göre, ağ saldırıları son üç yılın en yüksek seviyesine ulaşmıştır. Rapor, gelişmiş siber tehditlerin %33 oranında arttığını ortaya koymuştur(NCS, 2022).

Güvenlik uzmanları, işletmelerin hibrit iş gücüne geçişinin saldırı sayılarını artırdığını ve kurumlar için daha fazla potansiyel güvenlik açığı yarattığını belirtmektedir. Bununla birlikte, işletmeler BT sistemlerini düzenli olarak güncellemek ve güvenlik açılarını düzeltmek gibi basit ama kritik öneme sahip önlemleri uygulayarak siber saldırganları engelleyebilecektir (NCS, 2022).

Allianz 2020 raporuna göre işletmeler için siber riskler küresel ölçekte en büyük tehlike olarak sıralanmıştır(Allianz, 2020; Hoppe vd., 2021). Siber saldırılar, bir bilgi sistemi içinde bulunan kritik verileri çalmak, değiştirmek veya yok etmek amacıyla bilgi sistemini veya bilgisayar ağını hedef alan saldırılardır. Saldırganlar genellikle yetkisiz erişim elde eden herhangi bir kişi, grup veya süreç olabilmektedir. Siber saldırılar kötü amaçlı yazılım kullanarak bilgi sistemindeki verileri/bilgileri, yazılım kodunu değiştirerek sistemi ele geçirmeye çalışmaktadır. Bu durum, yıkıcı etkilere ve verilerin/bilgilerin tehlikeye girmesine yol açmaktadır (Biju vd., 2019).

Literatürde sıklıkla tanımlanan bazı siber saldırı türleri vardır. Bunlar, zararlı yazılımlar, hizmet engelleme saldırıları, sosyal mühendislik saldırıları, oltalama saldırıları, SQL enjeksiyon saldırıları ve istenmeyen e-postalardır.

1.5.1. Zararlı Yazılımlar

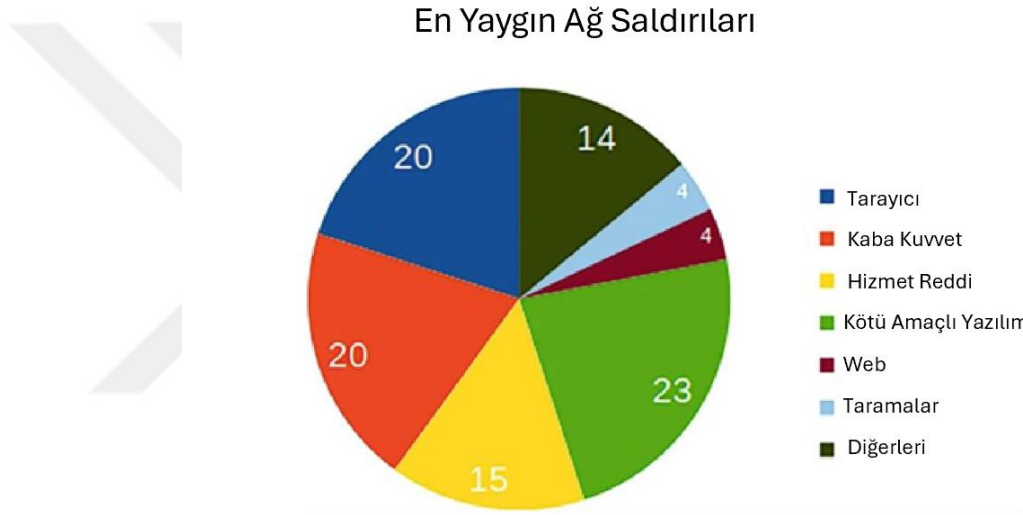
Zararlı yazılımlar bilgisayar sistemini kötü amaçla kullanmak için sistem bilgilerine erişim sağlamaya yardımcı olan ya da bilgisayar sistemlerine ciddi hasarlar veren bilgisayar programlarıdır. Zararlı yazılımlar şemsiye bir kavram olup birden çok alt kategoriye ayrılmaktadır. Bunlardan virüsler, solucanlar, truva atları, casus yazılımlar ve reklam yazılımları en bilinen zararlı yazılımlardır. Kötü amaçlı yazılımlar insanlara,

süreçlere ve teknolojilere zarar vermek için kullanılabilir. Fakat en önemli amaçları sistemlere yetkisiz erişim hakkını elde etmek ve kritik bilgilerin ele geçirmektir.

Kötü amaçlı yazılım saldırıları, kullanıcının kişisel veya iş bilgisayarına/sistemine izni olmadan virüs, solucan gibi kötü amaçlı yazılımların yüklendiği saldırılardır. Bu yazılımlar aracılığıyla sistem kesintiye uğratarak önemli bilgiler çalınmaktadır. Günümüzde bu yazılımlar kişisel hedeflerden daha çok ticari ve finansal hedefler için gerçekleştirilmektedir.

Şekil 9

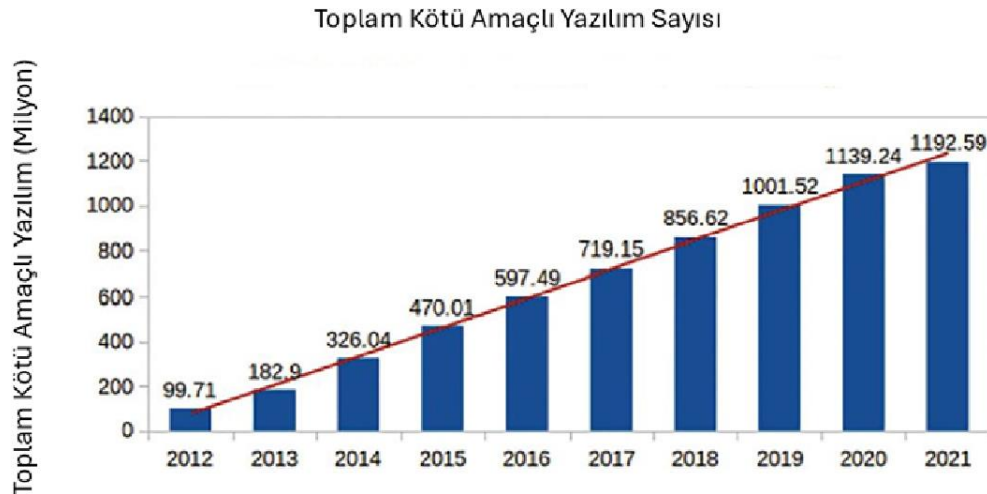
Siber Saldırı Türleri



Kaynak:(Kumar vd., 2022)

Şekil 10

Zararlı Yazılımların Oranı



Kaynak:(Kumar vd., 2022)

1.5.2. Virüsler

Bilgisayarlar, kullanıcı tarafından verilen talimatları birbiri ardına yürütmek için tasarlanmıştır. Bu talimatlar hesaplamalar yapar, veri tabanlarını korur, kullanıcılarla ve diğer sistemlerle iletişim kurar genellikle yararlı işler yerine getirirler. Ancak bazen, yürütülen talimatlar doğası gereği zarar verici ve kötü amaçlı olabilmektedir. Bu bilinmeden gerçekleştiğinde ilgili kodda bir yazılım hatası olarak olarak nitelendirilmektedir. Fakat istenmeyen davranışın gerçekleşmesini amaçlayan bir kişi tarafından oluşturulan kötü amaçlı kodlama içeren talimatlar olduğunda dikkat edilmelidir. Bir virüsün temel bileşeni, yürütüldüğünde kendisini daha önce etkilenmemiş diğer programlara veya dosyalara yayan bir dizi talimattır. Tipik bir bilgisayar virüsü iki işlevi yerine getirir. İlk olarak, kendisini daha önce bulaşmamış programlara veya dosyalara kopyalar. İkincisi, belirli sayıda yürütmeden sonra veya belirli bir tarihte virüsü kodlayan kişinin amaçlarını içeren diğer yönergeleri işletir. Virüsü yazan kişinin amaçlarına bağlı olarak, bu talimatlar bir mesajın görüntülenmesi, dosyaların silinmesi veya saklanan verilerin değiştirilmesi dahil olmak üzere birçok şeyi yapabilir. Bazı durumlarda, bir virüs hiçbir zararlı veya bozucu talimat içermeyebilir. Bunun yerine, kendini kopyalayarak ve disk alanı, işlemci hızı veya ağ bağlantıları gibi sistem kaynaklarını ele geçirerek hasara neden olabilmektedir (Wen, 1998).

Başka bir tanıma göre bilgisayar virüsü, genellikle kullanıcının bilgisi ve izni olmadan bir bilgisayar sistemine giren ve bilgisayarda depolanan verilerde yetkisiz ve istenmeyen değişikliklere neden olan bir bilgisayar programı veya kodudur. Bilgisayar virüsü kullanıcı bilgisayarına yasa dışı zarar verici faaliyetler yapan yazılım, kod ve kod blokları olarak ifade edilebilir. Fakat hasara neden olan her yazılım virüs değildir. Bazı yazılımlar, düzeltilmemiş veya fark edilmemiş hatalar nedeniyle sisteme zarar verebilir(Khan, 2012).

Bilgisayar virüsü terimi türetilmiştir ve bir anlamda biyolojik bir virüse benzemektedir. Latince kökenli virüs kelimesinin anlamı aslında zehirdir. Biyolojik virüsler kendisini daha büyük bir organizmanın hücrelerine enjekte ederek yayılır. Hücre daha sonra enfekte olur ve virüsün kopyalarını üreten biyolojik bir fabrikaya dönüşür. Bilgisayar virüsleri, biyolojik virüslerin bazı özelliklerini paylaştığı için virüs olarak adlandırılır. Bir bilgisayar virüsü, biyolojik bir virüsün insandan insana bulaşması gibi bilgisayardan bilgisayara bulaşır (Khan, 2012). Biyolojik virüse benzer şekilde bilgisayar virüsü, etkinleştirildiğinde kendisini veya kendisinin değiştirilmiş bir versiyonunu ana bilgisayar programına kopyalayacak tipik olarak 200-4.000 bayt kapasiteli bir makine kodudur. Bu

virüslü programlar çalıştırıldığında, kod yürütülür ve virüs daha da yayılır(Spafford, 1994).

Virüsler, kullanıcının bilgisi dışında ve izni olmadan bilgisayar işlemlerini olumsuz yönde etkileyen bir kötü amaçlı bir programlardır ve bilgisayarın işletim sistemine ve bilgisayardaki dosyalara zarar verebilmektedir. İlk bilgisayar virüsü 1981 yılında ortaya çıkmıştır. Elk cloner ismi verilen bu virüs o dönemde bilgisayarlara takılan disket sürücü aracılığıyla yayılmıştır(Shaukat vd., 2020, s. 7; Spafford, 1994).

Bilgisayar virüsü terimi literature ilk kez 1983 yılında Dr. Cohen tarafından “kendi kendini yeniden üretebilen programlar” şeklinde tanımlanmıştır. O sırada Dr. Cohen, Güney Kaliforniya Üniversitesi'nde bir güvenlik seminerine katılan yüksek lisans öğrencisidir. Derste kendi kendini yeniden üreten kod hakkında gösterdiği basit bir örneği sunmuştur. Danışmanı Profesör Len Adleman, Cohen'in bu yazılım tipine bir bilgisayar virüsü demesini önermiştir. Dr. Cohen'in doktora tezi ve sonraki araştırmaları bilgisayar virüsleri üzerine yayınlanmıştır(Cohen, 1987; Spafford, 1994).

Bilgisayar virüsü, bilgisayara ağlar aracılığıyla veya disk, CD, DVD, USB flash bellek gibi cihazlar aracılığıyla bulaşan, bu sistemde kendini kopyalayarak ve çoğaltarak sistemin yavaşlamasına bazı işlevlerini yerine getirememesine hatta önemli verilerin silinmesine neden olan kötü amaçlı yazılımlardır. Bilgisayar virüsleri genellikle küçüktür, bir bilgisayardan diğer bilgisayara yayılmak ve sisteme müdahale etmek için tasarlanmıştır.

Bilgisayar virüsleri, BT sistemlerinin güvenliğine ve bütünlüğüne yönelik tehdittir. Diğer tehditler gibi, bilgisayar virüsü de programların veya verilerin kaybolmasına veya değiştirilmesine neden olabilir ve bunların gizliliğini tehlikeye atabilir. Diğer birçok tehdidin aksine, bilgisayar virüsü, doğrudan insan müdahalesi olmaksızın programdan programa, belgeden belgeye ve bilgisayar sisteminden bilgisayar sistemine yayılabilir. Bilgisayar virüsleri e-posta ekleri yoluyla da yayılabilir bu nedenle nereden geldiği ve kimin gönderdiği bilinmeyen e-posta virüs olabilmektedir. Ayrıca, virüsler resimlerin, videoların ekleri veya internet aracılığıyla bilgisayara indirilen dosyalarda sıklıkla karşımıza çıkmaktadır.

2 Kasım 1988'de C programlama dilinde kodlanmış internet virüsü ARPANET sistemini ele geçirmiştir ve birçok bilgisayar merkezi kapanmak zorunda kalmıştır. Bunlara NASA'nın laboratuvarı ve MIT'de dahildir. Daha sonraları bilgisayar virüsleri birçok

değişikliğe uğramış olup yeni virüslerin yapısı karmaşık, tespit edilmesi ve kaldırılması zordur(Wen, 1998). Bilgisayar virüsleri ilk çıktığı zamandan itibaren küresel bir sorun haline gelmiştir ve internet üzerinden çok daha hızlı bir şekilde yayılarak büyük hasarlara yol açmaktadır. Şirketler küresel elektronik ticareti yürütmek için internet teknolojisini giderek daha fazla kullandıkça bilgisayar virüsü ile karşılaşma olasılığı da artmaktadır. Kurumlar ve bireyler çoğunlukla internet ortamında olan bu eski ve yeni virüslerin artan tehdidiyle yüzleşmek için kapsamlı bir virüs koruma politikasına sahip olmaları gerekmektedir (Wen, 1998).

Bir virüsün yayılmasının iki yolu vardır: virüslü bir cd, dvd, usb bellek kullanmak veya virüslü bir programı çalıştırmak. Var olan tüm bilgisayar virüsleri bilgisayarda bir yerde yaşar. Çoğu virüs, bilgisayarı kapatana kadar bellekte etkin kalır bilgisayar kapatıldığında virüsü bellekten silinir ancak bulaştığı dosya veya diskten silinmez. Bilgisayar bir sonraki açılıшта, virüslü program yeniden etkinleştirilir ve kendisini daha fazla programa kopyalamaya başlar. Beş ana virüs türü vardır; Bunlar, önyükleme virüsleri, program virüsleri, gizli virüsler, çok biçimli virüsler, çok parçalı virüslerdir(Wen, 1998).

Önyükleme virüsleri, önyükleme bölümünü değiştirir ve en yaygın virüslerdir. Her sabit diskte, bilgisayarın başlatıldığında nasıl çalıştığını kontrol eden bir önyükleme bölümü vardır. Bir önyükleme virüsü, başlatma sırasında sabit diskten belleğe yüklenir ve diğer uygulamalara, diğer disklerle bulaşır veya yalnızca düşük performansla neden olur. Virüs yayılımı bilgisayar açıldığında ve sürücünüzde bir disket olduğunda başlamaktadır.

İkinci virüs kategorisi, program virüsleridir. Bu virüsler program dosyalarında yaşar. Bu virüs türü, sistem dosyayı çalıştırdığında belleğe yüklenir. Bir kez belleğe alındığında, virüs daha sonra yürütülen tüm programlara bulaşabilir. Daha sonra bu dosyalardan diğer program dosyalarına bulaşabilir.

Gizli virüsler adından da anlaşılacağı gibi saklanma özelliğine sahip olan virüslerdir. Gizli niteliklere sahip bir virüs, bir önyükleme bölümünde veya bir program dosyasında bulunabilmektedir. Bilinen gizli virüslerin çoğu, önyükleme virüsü türündedir. Virüs genellikle fark edilememek için dosya boyutlarını değiştirir.

Çok biçimli virüsler, her dosyada farklı görünen ve algılamayı zorlaştıran virüslerdir. Çoğalma işlemleri sırasında özelliklerini değiştirirler. Bu virüsler, anti-virüs programlarının dahi tespit etmesi en zor olanlardır.

Bilgisayara bu virüs türlerinden herhangi birinin bulaşmış olabileceğine dair birkaç işaret vardır. Bu virüsler, bilgisayar ekranında alışılmadık grafikler veya mesajlar gösterebilmektedir. Ek olarak, bu virüsler kullanıcıdan habersiz sabit diskleri yeniden biçimlendirdiği, disk birim etiketini değiştirdiği ve bilinmeyen dosyalar veya alt dizinler oluşturduğu bilinmektedir. Hız ve bellek boyutu dâhil olmak üzere bilgisayarların performansı etkilenmekte ve programlar/dosyalar silinebilmektedir(Wen, 1998)

1.5.3. Solucanlar

Ağa bağlı bilgisayarlar, bilgisayar solucanları da dâhil olmak üzere çeşitli kötü amaçlı yazılım türlerine karşı hassastır. Bilgisayar solucanı, kendini yeniden üreten ve ağ bağlantıları üzerinden yayılan kötü amaçlı yazılımdır. Bilgisayar solucanı genellikle bilgisayar dosyalarına bulaşmaz, ağdaki başka bir bilgisayarlara bulaşır. Bu durum, solucanın kendini kopyalaması özelliği ile yapılır. Solucan kendini kopyalama yeteneğini kopyasına geçirir ve oluşturulan kopya diğer sistemlere aynı şekilde yayılmaya devam eder. Solucanlar aynı virüsler gibi kendisini sürekli bilgisayardan bilgisayara kopyalayan ve sistemdeki-ağdaki kaynakları sömüren kötü amaçlı yazılım programıdır. Fakat bir noktada virüslerden farklıdır, bilgisayar solucanları, kendilerini çoğaltan ve arka planda çalışan bağımsız programlardır; virüsler ise bulaşmak için bir ana bilgisayar dosyasına ihtiyaç duyar (Hornetsecurity, 2022). Bilgisayar solucanı, herhangi bir insan etkileşimi olmaksızın kendini çoğaltabilir ve sisteme zarar vermek için kendisini bir yazılım programına bağlamasına gerek yoktur. Kontrolsüz bir şekilde çoğalmış olan solucanlar, sistem kaynakları tükendiğinde, görevler yavaşladığında veya durdurduğunda fark edilebilir. Virüslerin aksine, solucanlar bir ağa bağlıdır ve herhangi bir insan eylemine bağımlı değildir (Chen ve Robert, 2004). Bilgisayar virüsü, görünüşte masum bir belge veya uygulamanın içine gizlenerek bilgisayarlar arasında yayılan bir programdır. Solucan ise sistem üzerinde başka hiçbir şeye "bulaşmadan" çoğalan ve dolaşan bir programdır (Knight, 2006).

Bilgisayar solucanı terimi ilk olarak 1975'te John Brunner'ın "The Shockwave Rider" adlı romanında kullanılmıştır. Bu romanın kahramanı, veri toplayan bir solucandır. Bilgisayar biliminin ilk günlerinde solucanlar, bir sistemin güvenlik açıklarından yararlanmak için tasarlandı. Virüs bulaşan bilgisayarlara ciddi şekilde zarar vermek yerine, arka planda çoğalmaya devam ettiler. Ancak günümüzde bilgisayar solucanlarının amacı değişmiştir.

Bugün, saldırganlar genellikle kurbanlarının bilgisayarlarına tam erişim sağlamak için solucanları kullanmaktadır (Hornetsecurity, 2022).

2 Kasım 1988'de Morris solucanı birkaç saat içinde 6.000 bilgisayarı devre dışı bırakmıştır. Solucan, öğrenci olan Robert Morris tarafından yazılmıştır. Daha sonra yapılan araştırmalarda solucanı yazma nedenleri bulunamamıştır ancak solucanın kasıtlı olarak programlanmadığı kanaatine varılmıştır. 1989'da, WANK solucanı e-posta aracılığıyla yayılmış ve sistem hesaplarını ve şifrelerini ayrıca kullanıcı adı ve şifrenin aynı olduğu veya şifrenin boş olduğu hesapları bulmuştur (Chen ve Robert, 2004).

1.5.4. Truva Atları

Virüsler veya solucanların aksine Truva atı, kendini kopyalamaz ve bilgisayarın kontrolünü ele geçirebilen bir tür kötü amaçlı yazılım veya kodlardır. Truva Atı, verileri bozmak, çalmak veya BT ağ sistemine zarar vermek, gibi kötü eylemlerde bulunmak için tasarlanmıştır. Truva atı, gerçek bir uygulama veya dosya gibi görünür fakat yazılım cihaza yüklenmesi ve çalıştırılmasıyla sisteme zarar vermeye başlamaktadır. Truva Atı yazılımı kurulduktan sonra tasarlandığı eylemi gerçekleştirebilir (Shelly ve Vermaat, 2012, s. 288).

Truva atı, bazen Truva atı virüsü olarak da adlandırılmaktadır ancak bu yanlış bir isimlendirmedir. Virüsler kendilerini çalıştırabilir ve çoğaltabilir. Truva atları ise bir kullanıcıya ihtiyaç duyar, kullanıcının Truva atlarını çalıştırması gerekir. Bilgisayar virüsleri, solucanlar ve sahte güvenlik yazılımlarının aksine, truva atları genellikle kendilerini başka dosyalara kopyalamaya veya yayılmaya çalışmazlar(Johansen, 2020).

1.5.5. Hizmet Engelleme (DOS/DDOS) Saldırıları

Dijital dünyada, internet, çok sayıda hizmet sunan hayati bir kaynak haline gelmiştir. Bu hizmetlerin herhangi bir nedenle kullanılamaması, toplum ve devlet üzerinde çok ciddi mali sonuçlara yol açmaktadır. Siber dünyadaki en yıkıcı saldırılardan biri DOS (Denial of service) ve DDOS (Distributed denial-of-service) saldırılarıdır. DOS saldırılarında saldırgan internet'e bağlı bir ana bilgisayarın hizmetlerini geçici veya kalıcı olarak kesintiye uğratarak bir makineyi veya ağ kaynaklarını gizli istemcilerin kullanımına açmaya çalıştığı bir siber saldırıdır. İnternette DOS saldırılarını başlatmanın iki yöntemi vardır. Bunlardan birincisi, saldırgan kötü niyetli paketler göndererek kurbanın makinesinde çalışan protokolü veya uygulamayı gizler. İkincisi, saldırgan, kurbanın

makinesinin tüm kaynaklarını almak ve kullanıcılarla etkileşime girmesini engellemek için büyük bir işe yaramaz paket trafiği gönderir(Zargar vd., 2018).

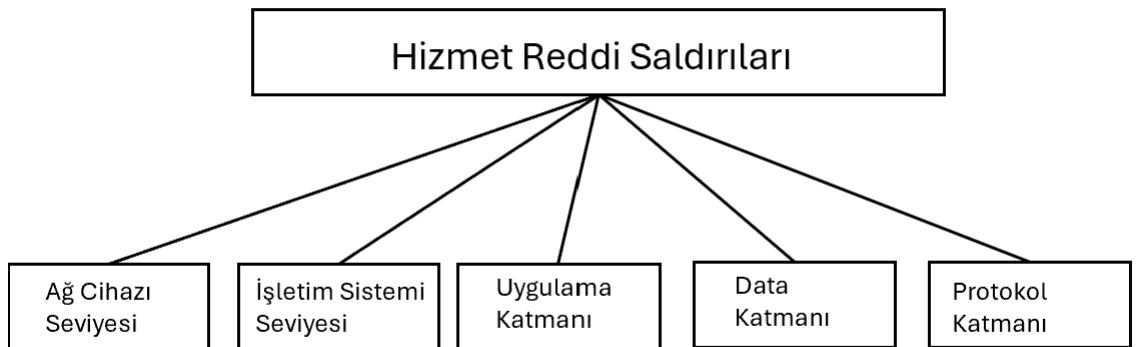
Hizmet Reddi (DOS) saldırılarının temel amacı, hizmeti bozmak veya zarar vermek yerine bir makineye veya hizmete erişimi sınırlamaya çalışarak hizmetlerin kesintiye uğramasıdır (Douligeris ve Mitrokotsa, 2004). Hizmet Reddi (DOS) saldırıları, hedef sistemi kullanıcılar için kullanılamaz hale getirmeye çalışır. Saldırgan çok fazla sayıda erişim isteği (bir aşırı yük saldırısı) göndererek sistemin çökmesine veya başka bir şekilde yanıt vermemesine neden olmaktadır. Bu saldırı tiplerinde sistem kusurlarından yararlanılır ve saldırı sonucunda sistemde fiziksel hasara oluşabilmektedir. Odak noktası, ağa bağlı bir bilgisayarı kullanıcıları için erişilemez hale getirmeye çalışmaktır (Douglas vd., 2017).

En yaygın DOS saldırıları, bilgisayar ağının bant genişliğini veya bağlantısını hedefler. Bant genişliği saldırıları, ağı o kadar yüksek hacimli bir trafikle doldurur ki, mevcut tüm ağ kaynakları tüketilir ve kullanıcı istekleri geçemez, bu da verimliliğin düşmesine neden olur. Bağlantı saldırıları, bir bilgisayarı yüksek hacimli bağlantı istekleriyle doldurur, mevcut tüm işletim sistemi kaynakları tüketilir ve bilgisayar artık kullanıcı isteklerini işleyemez hale gelir (Douligeris ve Mitrokotsa, 2004).

DOS saldırıları, *Şekil 11*'de gösterildiği gibi saldırıya uğrayan protokol seviyesine göre beş kategoride sınıflandırılabilir.

Şekil 11

Hizmet Reddi Saldırılarının Sınıflandırılması



Kaynak: (Douligeris ve Mitrokotsa, 2004).

Ağ aygıtı düzeyindeki DOS saldırıları, yazılımdaki hatalardan veya zayıflıklardan yararlanmak veya ağ cihazlarının donanım kaynaklarını tüketmeye çalışmaktan kaynaklanabilecek saldırıları içerir.

İşletim sistemi düzeyinde DOS saldırıları, işletim sistemlerinin protokolleri uygulama yollarından yararlanır.

Uygulama tabanlı saldırılar, hedef ana bilgisayarda çalışan ağ uygulamalarındaki belirli hatalardan yararlanarak veya kurbanlarının kaynaklarını tüketmek için bu tür uygulamaları kullanarak bir makineyi veya hizmeti arızalı duruma getirmeye odaklanılır. Saldırgan uzak ana bilgisayardaki tüm mevcut kaynakları tüketmek için bunları kullanması da mümkündür.

Veri saldırıları, saldırgan büyük miktarda veri göndererek ve bilgisayarın veya ağın büyük miktarda veriyi işlemesine neden olarak, bir ağ, ana bilgisayar veya cihaz için mevcut olan bant genişliğini en geniş ölçüde kullanmaya çalışır.

Protokol özelliklerine dayalı DOS saldırıları, belirli standart protokol özelliklerinden yararlanır. Örneğin, bazı DOS saldırısı türü DNS'ye odaklanmıştır ve DNS ön belleğine saldırmayı içerir.

Geleneksel olarak, DOS saldırıları tek bir kaynaktan başlar, ancak daha sonra dağınık bir şekilde devam eder bu nedenle Dağıtılmış Hizmet Reddi saldırıları (DDOS) olarak adlandırılır. DDOS saldırısı, bir veya daha fazla kurbanı karşı saldırıyı başlatmak için birçok bilgisayar kullanır. Saldırının doğası gereği tespit edilmesi zor olmaktadır (Kaur Chahal vd., 2019).

DOS'un bir uzantısı olarak, DDOS saldırıları, belirlenen hedefleri kullanıcılar tarafından erişilemez hale getirmek için çok sayıda koordineli saldırganlar ile gerçekleştirilir. Saldırımı gerçekleştiren yazılımlar, onları çalıştıran sistemlerin sahipleri tarafından açık bir şekilde başlatılabilir ve kontrol edilebilir veya kullanıcının bilgisi olmadan sistemler üzerinde gizlice çalışıyor olabilir. Bu genellikle, bir sistemin güvenliğinin kötü amaçlı yazılımlar tarafından veya yetkisiz yazılımların üzerinde çalışmasına izin vermek için güvenlik açıklarından yararlanan üçüncü taraf tarafından tehlikeye girmesinin sonucudur (Douglas vd., 2017).

İlk DDOS saldırısı 1999 yılında bir saldırganın Minnesota Üniversitesi'nin bilgisayar ağını iki gün boyunca erişime kapatmasıyla başlamıştır. 2000 yılında düzenlenen DDOS

saldırısı, Ebay, Yahoo, Amazon ve CNN dahil olmak üzere ünlü web sitelerinin erişim engeline neden olmuştur. Bu olaydan sonra, DDOS olaylarının sayısında hızlı bir artış yaşanmıştır. Günümüzün DDOS saldırılarında saldırganlar, saldırıyı başlatmak için daha karmaşık yöntemler kullanmaktadır. Saldırıları azaltma ve tespit tekniklerinin artmasının yanı sıra eş zamanlı olarak saldırı boyutu ve sıklığı hızla artmaktadır(Zargar vd., 2018).

DDOS saldırganları çok sayıda ve çeşitli nedenlerle gerçekleştirilir. Bu nedenler aşağıdaki kategorilerde sınıflandırılır:

Finansal Kâr: Saldırganlar, finansal kazanç için herhangi bir kurumu hedef alır. Bu kategorideki saldırganlar en tehlikeli ve deneyimli olanlardır. Bu saldırıları önlemek veya savunmak zordur.

Kişisel Sorunlar: Kişisel intikam veya adaletsizlik gibi duygulara sahip saldırgan saldırı başlatabilir.

Tanıtım: Bu kategorideki bir saldırganın amacı, internet üzerinde popülerlik kazanmak ve bir gazete manşeti olmak için saldırı yapmaktır.

Deney yapmak: Bir saldırının nasıl başlatıldığını öğrenmek için ön saldırı denemesi yapılabilmektedir.

Siber savaş: Saldırgan, başka bir devletin veya uluslararası bir şirketin bilgisayarına veya bilgi sistemine saldırmaya çalışan bir devlet veya uluslararası bir kuruluştur.

İdeolojik inanç: Saldırgan, ideolojik inançlarından dolayı saldırı düzenleyebilmektedir. Örneğin, politik güdüler bir DDOS saldırısının başlatılmasına yol açabilmektedir (Hoque vd., 2014; Zargar vd., 2018).

1.5.6. Sosyal Mühendislik

Sosyal mühendislik, insan zayıflığından yararlanma yoluyla bir hedef hakkında bilgi toplamanın en basit yöntemlerinden biri olarak tanımlanmaktadır(Conteh ve Schmick, 2016). Genel olarak, sosyal mühendislik, hedefleri kasıtlı olarak manipüle etmek için aldatıcı tekniklerin tasarımı ve uygulanması anlamına gelir. Siber güvenlik bağlamında sosyal mühendislik, öncelikle mağdurları gizli verileri ifşa etmeye veya güvenlik protokollerini ihlal eden, gizli bilgileri açığa çıkaran eylemler gerçekleştirmek için kullanılır. Bir sosyal mühendislik saldırısının temeli, en zayıf halka yani bireyleri hedef almaktadır(Breda vd., 2017).

Tarih boyunca sosyal mühendisliğin çeşitli biçimleri görülmekteydi, ancak günümüz dünyasında teknolojinin yaşamın her alanında artan kullanımı göz önüne alındığında, bu tehdit büyümeye ve durdurulması zor hale gelen karmaşık bir sürece dönüşmeye devam etmektedir. Aslında, sosyal mühendislik, teknik olmayan yollarla yapılan bir siber saldırı türü olarak da ifade edilebilir. Sosyal mühendislik sistemlere odaklanmak yerine, organizasyonlardaki insan unsuruna odaklanır.

COVID-19 pandemisiyle birlikte sosyal mühendislik saldırılarında ciddi artış yaşanmıştır. Google, bir hafta içinde Gmail kullanıcılarına gönderilen 18 milyon kimlik avı e-postasını engellediklerini duyurmuştur (Sonnemaker, 2021). Kimlik avı, alıcının bir bağlantıya tıklaması, bir eki açması veya bazı bilgileri açığa çıkarmasını sağlayan sosyal mühendislik saldırısıdır(Washo, 2021)

1.5.7. Oltalama – Yemleme (Phishing) Saldırıları

"Phishing" sözcüğü ilk olarak 2 Ocak 1996 yılında, bir grup bilgisayar korsanı tarafından "America Online" kullanıcılarının kimlik bilgilerinin çalınmasını Usenet haber grubunda duyurulmasıyla ortaya çıkmış en eski siber saldırı türlerinden biridir. 1990 yıllardan tarihten itibaren kimlik avı saldırılarının ölçeği ve karmaşıklık derecesi gün geçtikçe artarak devam etmektedir(Orunsolu vd., 2022). "Phishing" kelimesi Türkçede kimlik av, oltalama veya yemleme olarak kullanılmaktadır. Kimlik avı saldırıları, bir tehdidi belirli bir ortam aracılığıyla kurbanın sistemine iletmek için mevcut bir güvenlik açığından yararlanarak değerli varlıkların hedef alındığı sosyo-teknik bir saldırı olarak tanımlanmaktadır(Alkhalil vd., 2021).

Oltalama veya başka bir deyişle kimlik avı saldırıları sosyal mühendislik saldırılarının özel bir biçimidir. Kimlik avı saldırısı, kurbanları kandırarak kişisel ve finansal veriler gibi hassas verilerini yönlendirilen alana girmeleri için tasarlanmıştır. Kullanıcıya zarar vermek veya bilgi elde etmek için kötü amaçlı ekleri olan veya URL'leri yeniden yönlendiren e-postalar, oltalama saldırılarının yaygın biçimleridir(Magdy vd., 2022).

Oltalama saldırıları en etkili ve en iyi bilinen siber saldırılardan biri olmakla birlikte kullanıcıların bilgilerini elde etmeye ve bilgi güvenliği ihlaline neden olmaktadır. Saldırganlar genellikle gerçek görünümlü sahte web siteleri, e-postalar ve sahte telefon numaraları gibi yöntemler kullanarak hedefteki kullanıcıyı yanıltarak saldırılar düzenlemektedir.

Kimlik avı ve zararlı yazılımlar en kritik saldırılar olarak kabul edilir(Martínez Torres vd., 2019). Oltalama saldırısı sırasında saldırganlar, hedef kullanıcıların kendileri hakkında bilgilerini açığa çıkarmak için dijital aldatmaca kullanır. Saldırının başarısı, saldırganların hizmetleri ve bağlantıları ne kadar iyi taklit ettiğine ve kullanıcının neyin sahte ve neyin gerçek olduğunu ne kadar iyi ayırt edebildiğine bağlıdır. Örneğin, bazı yazım hataları olan bir oltalama e-postası kullanıcı tarafından kolaylıkla fark edilebilir. Bilgisayar kullanıcıları kimlik avı saldırısına uğrarsa, kurumun güvenlik duvarı, şifreleme yazılımları veya iki faktörlü kimlik doğrulama mekanizmasına sahip olması bir fayda sağlamamaktadır(Hong, 2012).

Son yıllarda, evrensel düzeyde ağlar üzerinden gerçekleştirilen kimlik avı saldırıları önemli ölçüde artmıştır. Kimlik avı saldırıları, insanları dolandırıcılık amaçlı kurulmuş olan internet sitelerini ziyaret etmeye ve bu sitelere kişisel bilgilerini girmeye ikna etme sürecinden oluşur. Kimlik avcıları, kullanıcıları yanıltmak için genellikle web sayfalarını görsel olarak gerçek web sayfalarına benzer hale getirir(Purkait, 2012, s. 382).

Siber suçlular, hedeflerine ulaşmak için genellikle siber hijyen eksikliği olan veya teknik güvenlik açıklarına ek olarak yetersiz eğitim almış kullanıcıları hedef almaktadır. Kimlik avına saldırılarına karşı duyarlılık, bireyler arasında değişiklik gösterir, bu nedenle çoğu saldırıda, kimlik avcıları karmaşık teknolojiler kullanmak yerine insan doğasını kullanır(Alkhalil vd., 2021).

2016 yılında yayınlanan bir rapora göre, kimlik avı saldırılarının sayısı ülkelere göre karşılaştırılmıştır. Özellikle gelişmekte olan ülkelerde %47,09 oranı ile Çin ilk sırada yer almış olup %42,8 ile Türkiye ikinci sırada yer almıştır(APWG, 2016). 2021 yılında yayınlanan bir rapora göre ise 2021 yılının aralık ayında yaşanan saldırı sayısı 316.747 olarak kaydedilmiştir. Bu sayı bu zamana kadar görülen en yüksek sayı olarak kayıtlara geçmiştir. Ek olarak, oltalama saldırılarının sayısı 2020 yılına kıyasla 3 katına çıkmıştır(APWG, 2021).

2022 yılında yapılan bir araştırmaya göre, oltalama yani kimlik avı saldırılarının en yaygın siber güvenlik ihlali olarak açıklanmıştır(Ell ve Gallucci, 2020). Bu saldırılar hem kurumları hem de bireyleri etkilese de, kurtarma maliyeti, itibar kaybı, yasalardan/yönetmeliklerden kaynaklı alınan para cezaları ve azalan üretkenliği içeren kayıplar kurumlar için çok önemli olmaktadır(Medvet vd., 2008).

Siber suçlular her zaman kendi çıkarları için felaketlerden ve sıcak olaylardan yararlanmaktadır. Covid-19 krizinin başlamasıyla birlikte, kimlik avcıları tarafından çalışanlara, sağlık tesislerine ve hatta genel halka karşı çeşitli kimlik avı ve kötü amaçlı yazılım saldırıları düzenlenmiştir(Microsoft, 2020) .

Kimlik avı veya oltalama saldırılarından kaynaklanan kayıplar, milyonlarca lirayı geçebilecek finansal kayıplarla sınırlı olmayıp, aynı zamanda müşteri ve itibar kaybına neden olmaktadır. Kimlik avı raporuna göre, başarılı kimlik avı saldırılarından kaynaklanan zararlar, üretkenlik kaybından nakit kaybına kadar bir çok alanda zarara neden olmaktadır. Daha özelde çalışanlardan kaybedilen saatler, olay müdahalesi nedeniyle zaman kaybı, itibarın zarar görmesi, fikri mülkiyet kaybı, doğrudan parasal kayıplar, müşteri kayıpları, yasal cezalar gibi etkileri olmaktadır(Proofpoint, 2020).

Literatürdeki araştırmalar kimlik avı saldırılarına karşı duyarlılık ile demografik değişkenler (örneğin yaş ve cinsiyet) arasındaki ilişkiyi ele almıştır. Herkes kimlik avına karşı duyarlı olsa da, araştırmalar farklı yaş gruplarının belirli saldırılara daha duyarlı olduğunu göstermiştir. (E. J. Williams vd., 2018) yaptıkları bir araştırmaya göre 18 ila 25 yaş aralığındaki katılımcıların, diğer yaş gruplarına göre kimlik avı saldırılarına karşı daha savunmasız olduğunu bulmuştur.

2020 yılında yapılan bir araştırmaya göre, 1.350 öğrenciye kimlik avı saldırıları göndererek lisans öğrencileri arasındaki tıklama oranlarını ve demografik özelliklerini incelenmiştir. Mühendislik, matematik, sanat ve sosyal bilimlere kadar çeşitli disiplinlerden öğrenciler katılan bu araştırmada öğrenci duyarlılığının kimlik avı farkındalığı, bilgisayarda geçirilen zaman, siber eğitim, yaş, akademik yıl ve üniversite bölümü gibi bir dizi faktörden etkilendiği ortaya çıkarılmıştır. En şaşırtıcı bulgu, kimlik avı bilgisine daha çok sahip olanların kimlik avı dolandırıcılığına daha duyarlı olmalarıdır(Diaz vd., 2020).

Bilgi eksikliği, farkındalık ve dikkatsizlik, kullanıcıları kimlik avı tuzağına düşürmenin yaygın nedenleridir. Çoğu kişi bilmeden şüpheli bir eki açmış veya sahte bir bağlantıya tıklamıştır. Bu nedenle, eğitime odaklanmak ve kullanıcıları bu tür saldırılarla karşı hazırlamak, kimlik avı saldırılarının etkisini en aza indirmek için temel unsurlardır.

Şekil 12

Oltalama Saldırıları



Kaynak: Yazar tarafından oluşturulmuştur.

Oltalama tekniği, yemin atıldığı balık avına çok benzer, şüpheli olmayan bir kullanıcının yemi yakalayıp tıpkı bir balık gibi ısırmasına benzetilir. Bu nedenle oltalama, yem ve kanca yöntemi olarak da bilinir(Emm, 2006). Genellikle yem ya bir e-posta ya da herhangi bir web sitesidir. Kullanıcı güvenilir bir web sitesinin gerçeğe çok yakın bir kopyası olan sahte siteye girebilmektedir. Sahte web sitesi, orijinaline çok benzeyen bir görünüme sahip olacak ve kullanıcı adı, şifre, kredi kartı bilgileri gibi hassas bilgileri isteyecektir. Kullanıcı bilgilerini girdiğinde, veriler kimlik avcısına gönderilir ve bu şekilde veriler kimlik avcısı tarafından kullanılır(Brody vd., 2007; Purkait, 2012, s. 383).

1.5.8. İstenmeyen E-posta (Spam)

E-posta, dünyanın herhangi bir yerinde internet erişimi olan herkese neredeyse anında erişim sağlayan hayati bir iletişim çeşidi olmuştur. Tüm alanlarda birincil, hızlı ve ucuz bir iletişim aracını temsil ettiğinden, e-postaların kullanım hacmi hızla artmaktadır. İstenmeyen e-posta veya istenmeyen ticari toplu e-postalar, son yıllarda internette önemli bir sorun haline gelmiştir. İstenmeyen posta gönderen kişi web siteleri, sohbet grupları olmak üzere çeşitli kaynaklardan e-posta adresleri toplamaktadır(Awad ve Foqaha, 2016). Küresel e-posta trafiğinin %77'sinden fazlasını istenmeyen e-postalar oluşturmaktadır ve her geçen gün daha büyük bir sorun haline gelmektedir. Bu e-postalar kullanıcıların zamanlarından çalmakta ve depolama alanlarını işgal etmektedir. Ayrıca, her gün 270 milyardan fazla e-posta gönderilmesine rağmen, bunların yaklaşık %57'si istenmeyen e-postalar oluşturmaktadır(Mageshkumar vd., 2022). İşte bu noktada siber güvenliğe yönelik bir başka tehdit de İngilizce de “spam” olarak nitelendirilen bu

istenmeyen e-postalardır. Bu istenmeyen e-postalar bir grup alıcıya toplu olarak gönderilir(Abdulhamid vd., 2017, s. 15650–15654). İstenmeyen e-postalar genellikle bir ürün veya hizmetin tanıtımını gösteren reklam içerikli mesajlardır(Jindal ve Liu, 2007, s. 1189).

Diğer bir tanımlamaya göre istenmeyen e-postalar, alıcıyla herhangi bir teması olmayan bir gönderici tarafından ayırım gözetmeksizin doğrudan veya dolaylı olarak gönderilen istenmeyen e-posta olarak tanımlanır. Spamları engellemek veya silmek çok fazla vakit almaktadır. Bu sorunu çözmek için artık çeşitli spam algılama yazılımları kullanılmaktadır. Spam algılama yazılımı günümüz çağında her kurum veya işletme için zorunlu bir faktör haline gelmiştir(Mageshkumar vd., 2022).

İstenmeyen e-postalar siber güvenlik için ciddi bir tehdit oluşturmakta ve kullanıcıların istenmeyen e-postalara göz atmak için geçirdikleri sürede büyük bir zaman kaybına neden olmaktadır. Ayrıca, spam e-postalar tarafından tüketilen bant genişliği ve büyük sunucu depolamasına ek olarak, kurumlar için mali kayıplara ve rahatsız edici bireysel kullanıcılara neden olmaktadır. Kötü amaçlı e-postaların başka bir türü, kimlik hırsızlığına yol açan kullanıcılardan hassas bilgiler almayı amaçlayan kimlik avı e-postalarıdır. İstenmeyen e-posta gönderenlerin hedefi bu e-postalar aracılığıyla kötü amaçlı yazılım yaymaktır. Kullanıcıların sahte web sitelerine yönlendirilmesine neden olan sahte bağlantılar e-posta içine yerleştirilmektedir. Bu saldırıda, sahte bağlantılar iyi bilinen web sitelerini simule eder ve böylelikle daha az şüpheli görünür(Magdy vd., 2022).

Spam, toplu gönderilen mesajlar, telefon numaraları, kötü niyetli web bağlantıları, trend olan hashtag'ler, gizli web bağlantılarına sahip resimler, sağlık tavsiyeleri, fidye yazılımları, borsa spam'ları, sahte reklamlar, sahte incelemeler, sahte haberler şeklinde çeşitli konularda olabilmektedir. Spam gönderenler kimlik avı, casusluk, siber zorbalık gibi yasa dışı faaliyetlerde bulunurlar. Genellikle spam gönderenler, spam yaymak için yasal hesaplar yerine sahte hesaplar ve otomatik botlar kullanır. Seçimler sırasında siyasi partiler, siyasi propaganda ve çevrimiçi kampanyalar yayarak insanları etkilemeye çalışırlar. Ayrıca, çevrimiçi kullanıcıların çalınan kişisel bilgilerini ve davranış kalıplarını analiz ederek çeşitli etik olmayan web siteleri/uygulamalar aracılığıyla kişisel öneriler de bulunmakta bir istenmeyen e-posta biçimidir(Bindu vd., 2018; Qi vd., 2018; Rao vd., 2021). Spam gönderen kişi veya gruplar, para kazanmak, bilgisayarları kontrol etme veya

bir kullanıcının kişisel bilgilerine erişim gibi faaliyetlerden bazı avantajlar elde etmektedir (Rao vd., 2021).

1.5.9. SQL Enjeksiyon Saldırısı

Hızı ve uygun maliyeti nedeniyle her türlü veriyi depolamak için veri tabanlarına ihtiyaç vardır. Veri tabanını kullanmanın avantajı, çeşitli eylemleri otomatikleştirmesi, kaynaklardan ve çalışma saatlerinden tasarruf sağlamasıdır. Örneğin, işlemleri manuel olarak yapmak yerine, kullanıcılar veri tabanında depolanan raporları ile işlem yapabilmektedir.

SQL veya Türkçe anlamı yapılandırılmış sorgu dili ilişkisel veri tabanlarıyla etkileşim için varsayılan dildir. SQL Injection ise genellikle SQL komutları üzerinden veri tabanı iletişimi olan sistemlerdeki hatalardan, güvenlik açıklarından yararlanan bir siber saldırı türüdür ve bu nedenle basit bir saldırı türü olarak kabul edilir. Uygulamalardaki hatalar, veri tabanında değişikliklere veya uygulamaya uygunsuz erişime neden olmaktadır. Saldırganlar SQL enjeksiyon saldırıları aracılığıyla bir sunucu bilgisayarın veri tabanında tutulan herhangi bir gizli veriyi alabilir ve kötü amaçlı komutlar girebilir (Batista vd., 2018). SQL enjeksiyon saldırıları, kod enjeksiyon saldırıları olarak bilinir ve kısaca kod enjeksiyonu komutları bir bilgisayar programına veya sisteme yazma tekniğidir (Mitropoulos ve Spinellis, 2007).

Siber güvenlik, dünyanın her yerindeki insanların hayatlarının her alanında karşı karşıya kaldıkları önemli ve zor görevlerden biridir. SQL enjeksiyonu, saldırganların bir veri tabanını saldırı düzenlemek için kullandığı ana yöntemlerden biridir. Bu tür saldırılar, web sitesindeki veya bir veri tabanı sunucusundaki güvenlik açıklarından yararlanır. Saldırgan bir veri tabanına yetkisiz erişim elde edebilir, verileri okuyabilir veya değiştirebilir, verileri diğer kullanıcılar tarafından kullanılamaz hale getirebilir ve hatta veritabanı sunucusuna zarar verebilmektedir.

SQL enjeksiyon, siber saldırganların müşteri bilgileri, ticari sırlar vb. gibi hassas verilere yetkisiz erişim elde edebildiği en popüler siber saldırılardan biridir. SQL enjeksiyon, yasal olmayan bir şekilde veri tabanına izinsiz giriş yapmak, veri tabanındaki bilgileri okumak, güncellemek veya silmek için kullanıcı giriş alanlarına kötü amaçlı SQL kodu enjekte ederek çalışır. SQL enjeksiyon, makine öğrenimi veya derin öğrenme teknikleri kullanılarak tespit edilebilir (Hosam vd., 2021). Bu saldırılar, kullanıcılardan girdi alan bu

girdiyi ve SQL sorgularını temel bir veri tabanına dahil eden herhangi bir web uygulaması için önemli bir tehdittir(Halfond vd., 2008).

SQL enjeksiyon SQL kodları arasına zararlı kodlar yerleştirerek sistemi manipüle etme işlemidir. Bu yöntem gerçekleştirilmesi çok basit bir siber saldırı yöntemi olmasına rağmen yıllardır güncelliğini hiç kaybetmemiştir. SQL enjeksiyon yöntemi ile kullanıcı adı ve şifre bilgisi gibi temel verilere gerek duyulmadan sisteme girebilmek mümkündür. Saldırgan elde ettiği bilgiler ile veri tabanındaki verilerin bir kısmı ya da tamamına erişebilmektedir. Veri tabanı sistem yöneticisinin şifresini ele geçirerek veri tabanını silebilir, sisteme erişimi kapatabilir ve ya elde ettiği verileri kullanarak çeşitli sitelerde ücret karşılığında verileri satabilmektedir(Boyd ve Keromytis, 2004).

SQL Enjeksiyon Saldırısına Karşı Alınması Gereken Önlemler

- Veri tabanında tablo alanlarındaki isimlerin özenle seçilmeli ve tahmin edilmesi kolay olmamalıdır.
- Web formlarında veri girişi yapılırken bu veriler doğrulanmalı ve girilen değerlerin uzunluğu kontrol edilmelidir.
- Kullanıcı veri tabanına veri girdikten sonra veri tabanına gönderilen sorgular filtrelenmeli ve zararlı olarak nitelendirilebilecek karakterler değiştirilmeli veya kaldırılmalıdır.
- SQL tabanlı web uygulamalarında kullanılan veri tabanını veri ekleme, silme, güncelleme gibi işlemler sadece yetkili bir kişi tarafından gerçekleştirilmelidir.
- SQL enjeksiyon saldırısında kullanılabilecek komutlar (ekle, sil, güncelle vb.) olası sızma girişimleri hakkında bilgi vermeyi engelleyecek bir fonksiyon ile filtreleme yapılmalıdır.
- Veri tabanında tanımlı olan yönetici hesaplarının sınırlı düzeyde yetkilere sahip bir kullanıcı hesabı ile çalıştırılmasına dikkat edilmelidir.
- Veri tabanında kullanılmayan saklı yordamlar ve yönetici hesapları kaldırılmalıdır.
- Sisteme kayıtlı nesnelere tam erişim verilmemeli, kullanıcı bazında yetkilendirme yapılmalıdır.
- Web uygulaması ve veri tabanı sunucularının bulunduğu sistem, donanım veya yazılımlar güvenlik duvarı ile olası siber saldırılara karşı korunmalıdır.

- Veri tabanına veri eklenmesinden sonra verilerin yedeklenmesi güvenlik için önemlidir(Avcı vd., 2021).

Son zamanlarda SQL enjeksiyon saldırılarına ve güvenlik açıkları sorununa ilgi gösterilmesine rağmen, önerilen birçok çözüm sorunun tam kapsamını ele almakta başarısız olmaktadır. Birçok SQL enjeksiyon türü ve bu temel türlerde sayısız varyasyon vardır. Bu nedenle, çözümlerin çoğu, olası SQL enjeksiyon türlerinden yalnızca bir alt kümesini algılamak veya önlemek için kullanılmaktadır(Halfond vd., 2008).

1.6. Siber Güvenlik Kültürü

Siber güvenlik kültürü, şirketin güvenlik imajı üzerinde önemli bir etkiye sahip olabilmektedir. Kültür her zaman davranışı yönlendirmektedir. Güvenliğe değer veren bir kültürde, çalışanlar tutum ve davranışlarını dikkat etmektedir. Liderler ve çalışanlar, siber güvenliğin yalnızca teknolojiye bağlı olmadığını aynı zaman da herkesin ortak sorumluluğuna bağlı olduğuna inandıklarında kurumu güvende tutmak için daha fazla çaba göstermektedirler. Çalışanların sahip oldukları güvenlik bilinci kurum için güçlü bir savunma hattı haline gelir. Siber güvenlik kültürü, kurumdaki çalışanlarda siber güvenlik davranışlarını teşvik eden tutumlar ve değerler olarak tanımlanmaktadır. Diğer bir tanıma göre, siber güvenlik kültürü, bireylerin organizasyon sistemleri ile etkileşimde bulunmak ve ilgili prosedürleri, günlük görev ve faaliyetleri yürütmek için edindikleri tutumları, inançları, değerleri ve bilgileri içeren organizasyon kültürünün bir alt kültürü olarak ifade edilmektedir. Temelde bu tanım, kültürü örgütler içinde alışılmış bir davranış olarak tanımlar. Sektörler ve alanlar arasındaki bu tanımlar arasındaki benzerlikler, bağlamdan bağımsız olarak, kurumların ve çalışanlarının belirli koruma davranışları sergilemeleri ve güvenlik kültürü beklentilerini yerine getirmek için yürürlükteki prosedürleri takip etmeleri beklendiğini göstermektedir(Uchendu vd., 2021).

Siber güvenlik kültürü kavramı, bir organizasyonun işgücünün siber güvenlikle ilgili tutumlarını, bilgilerini, normlarını ve değerlerini ifade eder. Bunlar, organizasyonun amaçları, yapısı, politikaları ve süreçleri tarafından şekillendirilir. İyi bir siber güvenlik kültürü, hem kültürün örgütsel belirleyicilerinin (politika, süreç, liderlik, sosyal normlar vb.) hem de kültürün bireysel belirleyicilerinin (tutumlar, bilgi, değerler vb.) kurumun siber güvenlik yaklaşımıyla uyumlu olmasıyla gelişir. Etkili bir siber güvenlik kültürü oluşturma özünü, kurumu teknoloji değil bireylerin veya işgücünün güvenli hale

getirdiğini kabul etmektir. Bireyler siber saldırılara en iyi tepki veren aynı zamanda siber güvenlik zincirlerinin en zayıf halkasıdır(Fowler ve Everard, 2021).

Siber güvenlik kültürü, dijital güveni arttırma, kurumun müşteriler nezdinde itibarını arttırmaya ve çalışan özgüvenini oluşturmaya yardımcı olur. Organizasyonların daha az çabayla daha güvenli bir şekilde çalışabilmesi için iyi bir siber hijyenin standart uygulama haline geldiği bir ortam oluşturmaları gerekmektedir. Siber Güvenlik Becerileri raporuna göre, işletmelerin yalnızca %11'i siber güvenlik bilincine sahip olmayan çalışanlara siber güvenlik eğitimi verdiği ortaya konmuştur. Fakat artık günümüz kurumları için siber güvenlik eğitimi ve kültürünün önemi giderek daha fazla kabul görmektedir(Fowler ve Everard, 2021).

1.7. Bilgi Güvenliği

Günümüz firmalarının karşılaştığı en büyük sorunlardan biri de bilgi güvenliğini sağlamadaki en zayıf halkanın çalışanların davranışları olmasıdır. Çalışanlar iş bilgilerini arkadaşlarla paylaşmak, özel bilgileri arkadaşlara ve aileye söylemek, fikri mülkiyeti rakiplere satmak, kredi kartı bilgilerini çalmak ve gizli bilgileri kamuya ifşa etmek gibi bilgi güvenliğini ihlal eden davranışlar gerçekleştirebilmektedir (Y. J. Li ve Hoffman, 2023, s. 139; Willison ve Warkentin, 2013). Clearswift Insider Threat Index 2018 raporuna göre, kurumda bilgi güvenliği ihlallerinin %75'i çalışanları, müşterileri, eski çalışanları ve tedarikçilerinden kaynaklandığını ortaya çıkmıştır (Clearswift, 2018). Crypsis Group tarafından yayınlanan bir başka raporda, siber saldırıların %57'sinin kariyerlerinde ilerlemek isteyen ve ilgili kurumdan ayrılan çalışanlar tarafından gerçekleştirildiği belirtilmiştir (Crypsis, 2020).

Bilgi güvenliği farkındalığı (BGF), çalışanların kurumlardaki bilgi güvenliği politikalarının, kurallarının ve yönergelerinin önemini ne ölçüde anladığını ve davranışlarının bu politika, kural ve yönergelerle ne ölçüde uyumlu olduğunu ifade eder(Kruger ve Kearney, 2006; M. T. Siponen, 2000). McCormac vd. (2018) tarafından yapılan başka bir çalışmada herhangi bir işte çalışan bireylerin iş stresi ve bilgi güvenliği farkındalık düzeyleri arasında anlamlı bir ilişki olduğu ortaya çıkmıştır. Bu çalışmaya göre, çalışanların iş stresi ile baş edebildikleri veya iş stresine uyum sağladıkları zaman, siber güvenlik tehlikelerine karşı olan farkındalıklarının arttığı ortaya çıkmıştır (McCormac vd., 2018).

BÖLÜM 2. TEORİK ALTYAPI

Bu bölümde, siber güvenlik araştırmalarında sıklıkla kullanılan teorilere yer verilmiştir. Öncelikle siber güvenlik araştırmalarında en çok kullanılan teorilere değinilmiştir. Sonrasında tezin odak noktası olan Koruma Motivasyon Teorisi hakkında detaylı bilgiler verilerek ve eleştirel kaynak incelemesi yapılmıştır.

2.1. Siber Güvenlik Davranışına Yönelik Teoriler

Dijital cihazların ve verilerin/bilgilerin güvenlik yönlerini ifade etmek için kullanılan terminoloji son yıllarda önemli ölçüde değişmiştir. Bilişim teknolojilerinin ve internetin ilk ortaya çıktığı zamanlarda güvenlik kavramı bağlamında sıklıkla “Bilgisayar Güvenliği”, “BT Güvenliği” veya “Bilgi Güvenliği” “Ağ Güvenliği” kullanılmıştır. Fakat 2000’li yıllara gelindiğinde bu ifadeleri bir çatı altında toplayan şemsiye kavram olan “Siber Güvenlik” teriminin kullanılmaya başlanmasıyla yeni terminoloji giderek daha popüler hale gelmeye başlamıştır. Sonrasında hem uygulayıcıların hem politika yapıcıların “Siber Güvenlik” kavramını sıklıkla kullanılmasıyla daha da yaygınlaşmıştır (Schatz vd., 2017).

Siber güvenlik üzerine yapılan bibliyometrik makalede 1990 ve 2022 yılları arasındaki 4252 yayın incelenmiş olup siber güvenlik teriminin giderek artan bir kullanıma sahip olduğu bilgi güvenliği teriminin kullanımının gitgide azaldığı tespit edilmiştir (Karayel ve Akbıyık, 2023).

Siber güvenlik kavramının zaman içindeki kullanım sıklığını gösteren Google'ın arama trendlerinin yardımıyla görselleştirilen *Şekil 13* incelediğinde "Bilgisayar Güvenliği" ve "Bilgi Güvenliği" arama terimlerinin istikrarlı bir şekilde azaldığını, "Siber Güvenlik" teriminin kullanım sıklığının 2017 yılı itibari ile hız kazandığı görülmektedir. (*Şekil 13*).

Şekil 13

Siber Güvenlik, Bilgisayar Güvenliği ve Bilgi Güvenliği Trendleri



Kaynak: Yazar tarafından Google arama trendleri ile oluşturulmuştur (2004-2024).

Siber güvenlik genellikle teknik bir terim olarak nitelendirilse de aslında siber güvenliğin temel taşları hem teknik hem sosyal bilimlere içermektedir. Kullanıcı davranışlarını anlamak, güvenlik olaylarını ve veri ihlallerini tespit etmek için çok önemlidir. Güvenlik olayları ve ihlalleri zararlı yazılımların üretilmesi ve dağıtılması, saldırganların sosyal mühendislik kullanımının artması ve parola şifreleme gibi savunma davranışlarının eksikliği gibi insan faktörleri nedeniyle daha da kötüleşmektedir. Kullanıcılar ve siber saldırganlar olarak bireyler, siber güvenlik risklerinin ortaya çıkmasına, büyümesine, yayılmasına ve azaltılmasına katkı sağlamaktadır (King vd., 2018).

Kullanıcı hataları veya uzmanlık eksikliği siber saldırıların başlıca sebeplerindendir (Mohammad vd., 2022). IBM 2014 yılı raporuna göre, bilgi güvenliği olaylarının %95'inin insan hatasından kaynaklandığını bildirilmiştir. IBM'in 2021 raporuna göre ise, 2019'da 8,5 milyardan fazla kaydın ele geçirilmesinin temel sorumlusu içeriden gelen hatalar olduğu tespit edilmiştir (Singleton, C., DeBeck, C., ve Chung, 2021). Bu nedenle bireylerin evde ve işyerinde siber saldırılara karşı korunması için siber güvenlik davranışlarının teşvik edilmesi büyük önem taşımaktadır. Güvenli bir siber ortam sağlamak için siber güvenliğinin hem insan hem de teknolojik bileşenlerinin ele alınması gerekmektedir (Alsharida vd., 2023).

Siber güvenlik sistemi zayıflıklarının ana nedeninin insan hataları olduğu birçok bilim insanı tarafından savunulmaktadır (Alanazi vd., 2022; Pollock, 2017). Bu nedenle, başarılı bir siber güvenlik farkındalık kampanyasının temel taşı davranış değişikliğidir.

Siber güvenlik davranışının incelenmesi, insan hatalarından nasıl kaçınılacağı konusunda uzmanlara, profesyonellere ve kullanıcılara yeni bir bakış açısı sağlar. Siber güvenlik farkındalığı ve davranışı, çeşitli davranış ve öğrenme teorileri kullanılarak araştırılmaktadır. Planlı Davranış Teorisi (PDT), Genel Caydırıcılık Teorisi (GCT), Koruma Motivasyon Teorisi (KMT) ve Teknoloji Tehditlerinden Kaçınma Teorisi (TTKT) en bilinen ve en çok kullanılan teoriler arasındadır (Alsharida vd., 2023; Lebek vd., 2014; Sulaiman vd., 2022). Bu teoriler, siber güvenlik davranış araştırmalarında kullanıcıların davranışlarını açıklamak için yaygın olarak kullanılmıştır.

2.1.1. Koruma Motivasyon Teorisi

Rogers (1975) tarafından geliştirilen koruma motivasyonu teorisi (KMT), bireylerin kendilerini korumaya ve algılanan sağlık risklerine yanıt vermeye teşvik eden şeyler olarak tanımlanmıştır (Nazneen vd., 2022, s. 473). KMT, aslında bireylerin tehditlere karşı davranışsal tepkilerini değerlendirmek için oluşturulmuş teorik bir çerçevedir (Byrd vd., 2022, s. 2; Rogers, 1975). KMT 'nin en yaygın tanımı şu şekildedir: insanların kendilerini fiziksel, sosyal ve psikolojik tehditlerden korumak için belirli bir davranışın beklenen sonuçlarından kaynaklanan "korkuyu" azaltmaya çalışmalarıdır (Kim ve Han, 2019). KMT, bireylerin koruyucu davranışlarda bulunma niyetlerini tahmin etmek için tehdidin değerlendirilmesini ve tehditlerle başa çıkma değerlendirmelerini dikkate alır (Salazar vd., 2013).

Koruma motivasyonu teorisi, bireyin bir riski değerlendirme modelidir. Bu model, insanların yaşamlarını tehdit edebilecek herhangi bir riski bilişsel olarak nasıl algıladıklarını veya değerlendirdiklerini ve koruyucu davranışları veya önlemleri nasıl benimsediklerini açıklamaktadır. KMT, bireylerin koruyucu davranışlarda bulunma motivasyonuna ilişkin sosyal bilişsel model sunmaktadır (Gaston ve Prapavessis, 2014, s. 175). KMT, tehditlerle ilgili zararı ortadan kaldırmak için gerçekleştirilecek olan davranışları veya eylemleri incelemek ve analiz etmek için geliştirilen bir modeldir (Li vd., 2022, s. 2–3).

KMT modelinin temel bileşenleri, motivasyonel davranışı şekillendiren tehdit değerlendirme ve başa çıkma değerlendirme süreçleridir. KMT modelinde, tehdit değerlendirmesinin bileşenleri şunlardır:

Algılanan Önem: Kişinin bir tehdidin önemine ilişkin tahmini veya potansiyel zararın boyutuna dair algısıdır.

Algılanan Duyarlılık: Kişinin bir tehdidin ortaya çıkma olasılığına karşı algısıdır. Bireyler tehdidin ciddiyetini ve bu tehditten zarar görme ihtimallerini değerlendirir. Bu boyut, bireylerin tehdidin ciddiyetine ilişkin algısının davranışlarını bilişsel olarak etkilediğini belirtir.

Koruma motivasyonu teorisinin tehdit değerlendirme boyutu, siber güvenlik davranışını yönlendirmede etkilidir. Algılanan duyarlılık ve algılanan önem, olumlu siber güvenlik davranışlarını teşvik etmektedir (Mou vd., 2017). Bireyin tehditlere karşı duyarlılık algısı ne kadar yüksekse ve bu tehditlerin yansımalarının daha yüksek olduğunu düşünüyorsa siber güvenlik uygulamalarının benimsenmesi kuvvetle muhtemeldir. Bu nedenle tehdit değerlendirmesinin siber güvenlik davranışı üzerindeki etkisi çeşitli araştırmacılar tarafından incelenmiş ve tehdit değerlendirmesinin siber güvenlik davranışları üzerinde güçlü etkisi doğrulanmıştır (Bulgurcu vd., 2010; Burns vd., 2017; Li vd., 2010; Marett vd., 2011).

Tehditte başa çıkma değerlendirmesinde ise bireyler, yanıt yeterliliği, öz yeterlilik ve yanıt maliyeti olmak üzere üç bilişsel süreç aracılığıyla, tehdidin ortaya çıkmasını ortadan kaldıran veya en aza indiren önleyici tedbirleri benimser ve önleyici tedbirleri takip etme yeteneklerine güven duyarlar (Nazneen vd., 2022, s. 473).

Yanıt Yeterliliği: Bireyin önerilen koruma uygulamalarının tehdidi ortadan kaldırabileceğine dair beklentisidir.

Öz Yeterlilik: Kişinin tavsiye edilen eylem planını başarıyla uygulayabileceğine dair inancıdır.

Yanıt Maliyeti: Bireyin tavsiye edilen tepkiyi gerçekleştirmesinin ne kadar maliyetli olacağına dair inancıdır.

KMT'nin başa çıkma değerlendirme bileşeni, bireylerin siber güvenlik davranışlarını değiştirmede etkilidir (Doane vd., 2016). Literatürde öz yeterlilik ve yanıt yeterliliği ile siber güvenlik davranışı gerçekleştirme niyeti arasında pozitif ilişkiler olduğu bulunmuştur (Ifinedo, 2012; Vance vd., 2012). Abraham ve Chengalur-Smith (2019) tarafından yapılan çalışmada, katılımcılara verilen siber güvenlik eğitimi öz yeterlilikle ilgili web sayfalarının güvenliğini anlama davranışını önemli ölçüde etkilediği bulunmuştur. KMT'deki başa çıkma değerlendirmesinin üçüncü yapısı, bireyin güvenlik davranışlarıyla ilgili maliyetler hakkındaki algısı olan yanıt maliyetidir. Eğer siber güvenlik davranışı ile ilgili çaba ve zaman yüksekse, bireylerin siber güvenlik davranışını

gerçekleştirme olasılıkları daha düşük olacaktır. Literatürdeki araştırmalar yanıt maliyetinin siber güvenlik davranışı üzerindeki olumsuz etkisini doğrulamıştır (Khan vd., 2023; Mou vd., 2018).

Tehdit değerlendirme ve başa çıkma değerlendirme süreçleri, koruyucu davranışın teşvik edilmesine, sürdürülmesine ve yönlendirilmesine aracılık eder (Floyd vd., 2000). Süreç, bir tehdidin tehdit değerlendirme sürecini tetiklemesi ile başlamaktadır (Floyd vd., 2000). Burada bahsedilen tehdit bu çalışma kapsamında bir siber güvenlik tehdididir. KMT'nin bileşenleri açısından incelendiğinde: (1) Siber saldırı olayının algılanan önemi (örn. şüpheli bir e-posta ekini açmanın bir sonucu olarak kişinin bilgisayarına virüs bulaşması); (2) algılanan duyarlılık (örn. güvenlik önlemlerine yeterince dikkat edilmezse kurum bilgileri tehlikeye girebilir.); (3) yanıt yeterliliği (örn. önerilen siber güvenlik önlemlerini yerine getirme); (4) öz yeterlilik (örn. bir çalışanın öngörülen siber güvenlik önlemlerini başarıyla yerine getirebileceğine dair inancı) ve (5) yanıt maliyetleri (örn. siber güvenlik önlemlerini uygulamanın bir takım iş yükü ve zaman maliyetlerinin olması).

2.1.2. Teknoloji Tehditlerinden Kaçınma Teorisi

Siber güvenlikle ilgili insan faktörleri üzerine yapılan pek çok çalışma, BT kullanıcılarının güvenlik riskini azaltmaya yönelik önleyici/koruyucu eğilim ve davranışlarına odaklanmaktadır. Bu motivasyon faktörleri, ilk olarak 1975'te Ronald Rogers tarafından ortaya atılan Koruma Motivasyon Teorisi'nde yer almaktadır. KMT, daha sonra Liang ve Xue tarafından tekrar geliştirilerek, Teknoloji Tehditlerinden Kaçınma olarak adlandırılan teorik model ortaya konmuştur (Liang ve Xue, 2009).

Teknoloji tehditlerinden kaçınma teorisi(TTKT), risk analizi faktörünü (Baskerville, 1991), sağlık psikolojisi faktörleriyle (Rogers, 1983; Weinstein, 2000) birleştirilerek oluşturulmuştur (Liang ve Xue, 2010a, s. 396). TTKT, bireylerin bilişim tehditlerinden kaçınma davranışını inceleyen ve belirleyicilerini açıklamayı amaçlayan bir teoridir. Süreç teorisi olarak da nitelendirilen TTKT, bilgi teknolojileri kullanıcılarının kaçınma davranışlarının olumlu geri bildirim döngüsüyle açıklamaktadır. Döngü, bilişim tehditlerinin ortaya çıkmasıyla başlamaktadır. Daha sonra kullanıcılar kötü amaçlı olan bilgi teknoloji tehdidinin varlığından haberdar olur ve mevcut durumlarına ilişkin bir algı geliştirirler. Bilgi teknoloji tehdidinden zarar görmek anti-hedef (istenmeyen son durum) olarak belirlenir ve bu durum mevcut durumla karşılaştırılır. Mevcut durumlarının anti-hedefe çok yakın olduğu görüldüğünde bir tehdit duygusu geliştirilecektir. Tehdit,

bireyleri söz konusu tehditten kaçınmak için başa çıkma davranışını gerçekleştirmeye motive edecektir. Yani başa çıkma davranışı, nesnel veya öznel olarak mevcut durum ile istenmeyen son durum arasındaki farklılığı artırmak için gerçekleştirilir (Liang ve Xue, 2009, s. 77).

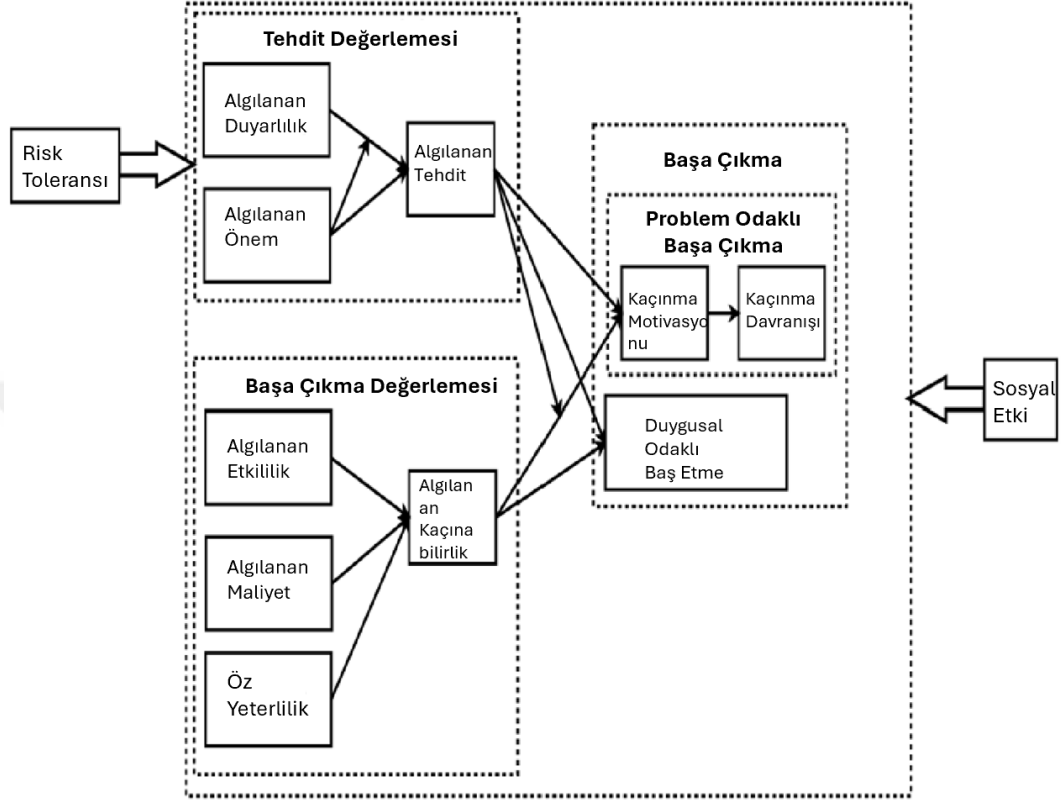
TTKT, kullanıcıların teknoloji tehditlerine ilişkin farkındalıklarını ve bunlardan kaçınma motivasyonlarını açıklamada geniş bir perspektif sunmaktadır (Al-Emran vd., 2023, s. 5). Tehdit ve başa çıkma değerlendirmesinin yanı sıra risk toleransı ve sosyal etkiyle ilgili faktörlerini de içermektedir (Gillam ve Foster, 2020, s. 2).

Teori, belirli bir bağlamda bireylerin tehdit algısının, belirli bir siber tehdidin ciddiyeti ve bu tehdide karşı duyarlılıklarına ilişkin görüşlerine dayalı olarak oluştuğunu öne sürmektedir. Bireyler daha sonra belirli bir tehditle başa çıkma yeteneklerini aşağıdakilere dayanarak değerlendirirler: 1) belirli bir önlemin tehditten kaçınmalarına yardımcı olmada ne kadar etkili olduğuna inandıkları, 2) kaçınma önlemini uygulamanın genel çaba maliyeti ve 3) uygulama yetenekleri koruma. Bu değerlendirme sürecinin çıktısı, belirli bir düzeyde kaçınma motivasyonudur ve bu da bireyin özellikle tehditten kaçınmasına yardımcı olmayı amaçlayan davranışlarda bulunma kararını etkilemektedir (Young vd., 2016, s. 8). Yapılan bir araştırmada TTKT, kullanıcıların siber güvenlik davranışlarını incelemek için uygun bir model olduğu bulunmuştur (Young vd., 2016).

TTKT, BT kullanıcılarının tehditten kaçınma davranışlarını etkileyen süreci ve faktörleri tanımlamaktadır (Liang ve Xue, 2009). Ayrıca iş dışı ortamlardaki güvenlik davranışlarının açıklanabileceği genel bir teorik çerçeve de sunmaktadır (Liang ve Xue, 2010a, s. 396). BT kullanıcıları öncelikle karşılaştıkları BT tehdidinin varlığını ve derecesini değerlendirir, ardından tehditten kaçınmak için neler yapabileceklerini değerlendirmektedir (Lazarus ve Folkman, 1984). Bu değerlendirmelere dayanarak tehdidi azaltmak için hangi koruma önleminin kullanılacağına karar verilmektedir. Bu süreçte kullanıcı algılarını, motivasyonlarını ve davranışlarını yansıtacak bir dizi temel faktör belirlenmiştir. TTKT' ne göre BT kullanıcıları, kötü amaçlı BT'nin bir tehdit olduğuna ve bir koruma uygulayarak önlenebileceğine inanırlarsa, kötü amaçlı BT'den korunacaklardır. Özetle, TTKT' ne göre, BT kullanıcıları tehdidin ne kadar önlenabilir olduğunu değerlendirmek için üç faktörü dikkate almaktadır. Bunlar kullanıcı bir koruma tedbiri alırsa - korumanın etkinliği, korumanın maliyetleri ve kullanıcının korumayı uygulama konusundaki öz yeterliliğidir (Liang ve Xue, 2010a, s. 396).

Şekil 14

Teknoloji Tehditlerinden Kaçınma Teorisi Modeli



Kaynak:(Gillam ve Foster, 2020, s. 2; Liang ve Xue, 2009, s. 79)

Teknoloji bireyler için insani ve sosyal açıdan fayda sağlarken diğer yandan bir tehdit oluşturabilmektedir. Teknoloji tehditlerinden kaçınma teorisine göre, kullanıcılar bilgi teknolojisi tehditlerinden kaçınmak istedikleri için yeni bir teknolojiyi kullanmak konusunda isteksiz olmaktadır. Bireyler, kullanılan teknolojiye bir tehdit olduğuna inanıyorlarsa birkaç koruma yöntemi uygulayarak bu tehditten kaçınmak isteyeceklerdir. Özetle, teknoloji tehdidinden kaçınma teorisi, bireylerin kötü amaçlı teknolojiye karşı olan duygularını ve bunun sonucunda onları bu teknolojiden kaçınmaya iten tehdit algısını ele almaktadır (Liang ve Xue, 2009, 2010b).

TTKT, çeşitli güvenlik olaylarında teknolojiyle ilgili tehditlerin anlaşılması ve ele alınması için değerli bir çerçeve sağlamaktadır. Liang ve Xue'ye (2009), kaçınma davranışını, kullanıcıların BT tehditleriyle nasıl başa çıkacaklarına karar vermek için tehdit değerlendirmesi ve başa çıkma değerlendirmesi olmak üzere iki bilişsel süreçten geçtiği dinamik, olumlu bir geri bildirim döngüsü olarak tanımlamaktadır.

TTKT modeli, algılanan duyarlılık, algılanan önem, algılanan tehdit, kaçınma motivasyonu, koruma etkinliği, koruma maliyetleri, öz yeterlilik ve kaçınma davranışından oluşan sekiz yapıyı ampirik olarak test eder ve kullanıcının risklere ve tehditlere karşı kaçınma davranışı hakkında değerli çıkarımlarda bulunur (Liang ve Xue, 2010a).

Teknoloji tehdidinden kaçınma teorisi, casus yazılımlar (Liang ve Xue, 2010; Young vd., 2016), kimlik avı saldırıları (Arachchilage ve Love, 2014) mobil güvenlik (Chen ve Li, 2017; Xin vd., 2022) ve internet güvenliği (Chen ve Liang, 2019; Y. Chen ve Zahedi, 2016) dahil olmak üzere bir çok araştırmada uygulanmıştır.

Bazı çalışmalar davranışsal ve organizasyonel faktörlerin kaçınma motivasyonu üzerindeki etkilerini ölçmek için TTKT modeline farklı modellerden ek faktörler eklemiştir (AlGhanboosi vd., 2023). Örneğin Verkijika (2019), kimlik avı tehditlerinden kaçınmak için pişmanlık faktörünün motivasyon üzerindeki etkisini ölçmek için TTKT modelini kullanmıştır. Ayrıca Forrester (2019), bilgi paylaşımının, bilgi güvenliği deneyiminin ve grup normlarının, tehditlerden kaçınma konusunda kullanıcıların motivasyonunu ve davranışını etkilediğini bulmuştur (Forrester, 2019).

2.1.3. Genel Caydırıcılık Teorisi

Genel caydırıcılık teorisi (GCT), potansiyel tehditlerin sonuçlarına ilişkin korku aşılayarak istenmeyen davranışlarda bulunmayı engellemeye odaklanan bir teoridir (Johnson vd., 2015). Cezalandırma tehdidinin veya olumsuz sonuçların bireyleri suç işlemekten veya saldırgan eylemlerde bulunmaktan caydırabileceğini ileri sürmektedir (Quackenbush, 2011, s. 743). GCT, ceza tehdidi veya olumsuz sonuçlar yoluyla potansiyel düşmanların istenmeyen davranışlarda bulunmasını engellemeye odaklanan bir kavramdır. Çalışanlar bağlamında GCT, belirli eylemlerin sonuçlarının, çalışanları bu eylemleri gerçekleştirmekten caydırabileceğini belirten bir teoridir.

Davranış psikolojisinin öne çıkan kavramlarından biri olan GCT, bireylerin istenmeyen davranışlarının ceza korkusuyla kontrol edilebileceğini veya önlenebileceğini öne süren bir teoridir (Gibbs, 1975; Kuhalampi, 2017, s. 9). Teori ilk olarak soğuk savaş boyunca askeri bir strateji olarak kullanılmıştır. Daha sonraki zamanlarda teori kriminoloji bağlamında suç işlemelerini önleyerek suçlu davranışlarını kontrol etmek için incelenmiş ve yüksek düzeyde korku cezasının bireylerin suç işleme niyetiyle olumsuz ilişkili olduğu bulunmuştur. İlerleyen zamanlarda organizasyonlarda çalışanların davranışlarını kontrol

edilmesi için GCT'nin faydalı olacağı fark edilmiştir. Böylelikle teori, organizasyonların kurallarıyla uyumsuz her türlü davranışı kontrol etmek ve önlemek için organizasyonlarda kullanılabilecek şekilde kullanılmaya başlanmıştır (Kuhlampi, 2017).

Her organizasyon çalışanların istenmeyen davranışlarını önlemek için bazı kurallar ve politikalar benimsemektedir. Ancak bu kurallar doğru şekilde uygulanmazlarsa, bireylerin davranışları üzerinde yalnızca küçük bir etkiye neden olacaktır (Peace vd., 2003). GCT, çalışanların istenmeyen eylemlerine karşı resmi yaptırım uygulamayı ve onları kurumsal politikalara uymaya yönlendirmeyi savunmaktadır.

Genel caydırıcılık teorisinin temelde üç bileşeni vardır. Bunlar; şiddet, kesinlik ve hız.

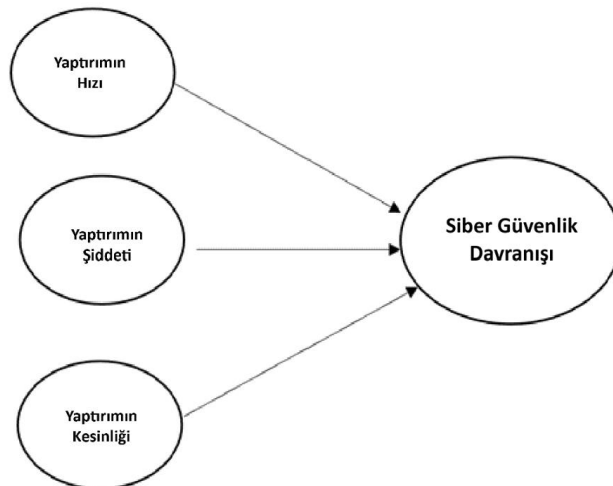
Yaptırımın Şiddeti: Ceza olarak da adlandırılan yaptırımın şiddeti, bir politikayı ihlal eden faaliyet gerçekleştirildiğinde algılanan yaptırımın ciddiyetine olan algıdır (Trang ve Brendel, 2019, s. 1267). Diğer bir ifadeyle yaptırımın derecesi olarak tanımlanabilir.

Yaptırım Kesinliği: Olağan dışı bir faaliyette bulunulduğu zaman cezalandırılma olasılığının algılanmasını ifade eder (Trang ve Brendel, 2019, s. 1267). Diğer bir ifadeyle yaptırımların uygulanma olasılığı olarak tanımlanabilir.

Yaptırım Hızı: Cezanın uygulanmasındaki algılanan hız olarak tanımlanmaktadır (Trang ve Brendel, 2019, s. 1267). Diğer bir ifadeyle yaptırımların uygulanma hızı olarak tanımlanabilir.

Şekil 15

Genel Caydırıcılık Teorisi



Kaynak: (Trang ve Brendel, 2019)

GCT, bireyler istenmeyen bir eylemde bulunduklarında bu davranışlarına yönelik belirli bir yaptırımın olması, yaptırımın bu davranışı caydıracak kadar şiddetli olması ve eylemin gerçekleşmesinden hemen önce uygulanması gerektiğini öne sürmektedir (Williams ve Hawkins, 1986). Yapılan araştırmalara göre yaptırım şiddeti ve yaptırım kesinliğinin caydırıcılık teorisinde öne çıkan etkili iki bileşeni olduğunu göstermektedir. Fakat yaptırım hızının ise yetersiz ampirik analiz nedeniyle göz ardı edilen bir faktör olduğunu göstermektedir (Nagin ve Pogarsky, 2001). Çeşitli araştırmalarda ise, yaptırımların ciddiyetinden ziyade yaptırımların kesinliğinin çalışanların güvenlik politikalarına uyma niyetleri üzerinde olumlu bir etkisi olduğunu ortaya koymuştur (Herath ve Rao, 2009a, 2009b).

Caydırıcılık teorisi, çalışan davranışlarına ilişkin bilgi sistemi güvenliği araştırmalarında en çok kullanılan teorilerden biridir (D'Arcy ve Herath, 2011). Güvenlik davranışını kontrol etmek için çok fazla alternatif teori yoktur. Bu nedenle caydırıcılık teorisi bu bağlamda kullanılabilecek en güçlü teori olarak görülmektedir (Kuhlampi, 2017). Çalışan bir bireyin kurum bilgi sistemini kötüye kullanması bilgi güvenliği politikalarını ihlal ettiği anlamına gelir (Herath ve Rao, 2009b). Bu teoriye göre cezalandırılma olasılığı ne kadar yüksekse ve yaptırımlar ne kadar güçlüyse BT kullanıcıları o kadar iyi davranmaktadır (Herath ve Rao, 2009). Böylelikle güvenlik ihlallerinin sayısı azalacaktır. Bu şekilde politika ihlallerinin sayısı daha az olacaktır (D'Arcy ve ark. 2009).

D'Arcy vd. (2009), güvenlik eğitimi programlarının çalışanların güvenlik farkındalığını artırdığını bulmuştur. Bulgurcu vd. (2010), güvenlik farkındalığı programlarının, bireyin bilgi güvenliği hakkındaki inançlarını etkileyerek politika uyumu üzerinde dolaylı bir etkiye sahip olduğunu öne sürmektedir. Bulgurcu vd. (2010) çalışanların ne yapmaları gerektiğini tam olarak bilmelerini sağlamak için güvenlik eğitimlerinin düzenlenmesi gerektiğini öne sürmektedir.

Bilişim sektörü çalışanlarının güvenlik davranışlarının önemini ve neden olabileceği olası risklerinin fark edilmesiyle birlikte caydırıcılık teorisini bu bağlamda kullanmak için akademik çalışmalar başlamıştır (D'Arcy ve Herath, 2011). Straub ve Nance (1990), güvenlik ihlali yapanların tespit edilmesinin ve cezalandırılmasının bilgisayar suçlarının miktarını azalttığını bulmuştur (Straub ve Nance, 1990). Ek olarak güvenlik farkındalığı artırma, yaptırımlar hakkında bilgi verme ve kabul edilebilir sistem kullanımı gibi caydırıcı unsurların yanı sıra cezalarla ilgili açık ifadelerin güvenlik sorunlarının sayısı üzerinde önemli bir etkiye sahip olduğu bulunmuştur.

2.2. Siber Güvenlikte Koruma Motivasyon Teorisi

Koruma motivasyonu teorisi, insanların potansiyel tehditlere karşı stresli durumlara nasıl tepki verdiklerini incelemektedir (Saeed, 2023). KMT, sağlık (Milne vd., 2000), psikoloji (Floyd vd., 2000), bilgi teknolojisi (Sun vd., 2020; Wall ve Warkentin, 2019) başta olmak üzere çeşitli disiplinlerde yapılan araştırmalarda kullanılmıştır. Bilgisayar ve bilgi güvenliği alanında, KMT, çalışanların ve son kullanıcıların dijital varlıklarını korumak için ek motivasyona ihtiyaç duydukları bilgi güvenliği bağlamları için uygundur. Son yıllarda, koruma motivasyon teorisi, siber güvenlik literatüründe, kullanıcıların siber güvenlik tehditlerine nasıl tepki verdikleriyle ilgili olarak kullanılmaya başlanmıştır (Saeed, 2023).

Siponen vd. (2009), çalışanların bilgi güvenliği politikalarına uyma niyetlerini etkileyen faktörleri araştırmak için koruma motivasyon teorisini kullanmıştır. Herath ve Rao (2009), koruma motivasyon teorisi ile caydırıcılık teorisini birbirine entegre teorik bir model geliştirerek çalışanların bilgi güvenliği politikalarına uyum davranışlarını incelemiştir. Bu çalışmada çalışanlar güvenlik politikalarını ihlal ettiklerinde yakalanma ihtimalinin yüksek olduğunu algılasa güvenlik politikalarına uyma olasılıkları daha yüksek olduğu bulunmuştur.

Johnston ve Warkentin (2010), çalışanlar üzerinde yaptığı çalışmada, yanıt yeterliliğinin siber güvenlik eylemlerini benimseme niyetleri üzerinde olumlu bir etkisi olduğunu bulmuşlardır. Ancak bazı araştırmacılar çalışanların yanıt yeterliliğinin siber güvenlik politikalarına uyma niyetlerini olumlu yönde etkilemediğini tespit etmiştir (Siponen vd., 2014; Vance vd., 2012). Bu farklı sonuçlar örneklem büyüklüğünün küçük olmasından dolayısıyla yordayıcılar ile siber güvenlik koruyucu davranışları arasındaki ilişkileri tespit etme gücünün düşük olmasından kaynaklanıyor olabilir. İkincisi, bazı çalışmalar tüm faktörleri tek bir modele dahil etmeye çalışmadan KMT yordayıcılarının alt kümelerine odaklanmaktadır. KMT modelinin bazı faktörleri birbiriyle ilişkili olduğundan, tüm çerçeveyi modellemeye çalışmadan her bir yordayıcının benzersiz katkısını değerlendirmek zordur. Son olarak, kriter ölçüsü olarak kullanılan güvenlik davranışının değerlendirilmesi genellikle çalışmalar arasında farklılık gösterir ve birçok çalışma, çalışanların mevcut davranışsal faaliyetlerini değerlendirmeye çalışmak yerine gelecekteki davranışsal niyetlerini ölçmeye odaklanır (Li vd., 2019).

Yoon vd. (2012), öğrencilerin bilgi güvenliği davranışlarını gerçekleştirmesini motive eden faktörleri incelemiştir. Araştırma, özellikle yanıt yeterliliği ve öz yeterliliğin öğrencilerin bilgi güvenliği niyetleri üzerinde güçlü bir etkisinin olduğunu göstermiştir. Algılanan güvenlik açığının ise bilgi güvenliği motivasyonu üzerinde önemli bir etkisinin olmadığı ortaya koyulmuştur. Ayrıca öznel normun bilgi güvenliği niyetleri üzerinde anlamlı bir etkisinin olmadığı bulunmuştur. Fakat güvenlik alışkanlıklarının bilgi güvenliğini niyetleri üzerinde önemli bir etkisi olduğu bulunmuştur.

Crossler ve Bélanger (2014), bireysel güvenlik davranışlarını incelemek için Koruma Motivasyonu Teorisi ve Birleştirilmiş Güvenlik Uygulamaları Enstrümanı (BGUE) kullanmıştır. Bu çalışmada, KMT'den türetilmiş faktörlerin BGUE üzerindeki etkisi test edilmiştir ve sonuçlar, algılanan önem, yanıt yeterliliği ve öz yeterliliğin güvenlik pratiklerini etkilediğini, algılanan kırılganlığın ise güvenlik pratiklerini olumsuz yönde etkilediğini göstermektedir. Ayrıca yanıt maliyetinin güvenlik pratikleri ile anlamlı bir ilişkisinin olmadığı bulunmuştur.

Siponen vd. (2014), çalışanların bilgi güvenlik politikalarına uyumunu açıklayan çoklu teoriye dayalı yeni bir model önermiştir. Paradigma olarak Koruma Motivasyonu Teorisi, Mantıklı Eylem Teorisi (MET) ve Bilişsel Değerlendirme Teorisi (BDT) kullanılmıştır. Araştırma, algılanan önemin, kırılganlığın, öz yeterliliğin, çalışanın bilgi güvenliği politikalarına uyma niyetine yönelik tutumunun ve normatif inançların, bilgi güvenliği politikasına uyma niyetini olumlu yönde etkilediği bulunmuştur. Bu çalışma, Finlandiya'da çalışan 669 katılımcı üzerinde yapılmıştır.

Johnston vd. (2015), dijital varlıklarına yönelik tehditlerle karşılaşan ve bunlara karşı politikaları uygulamak zorunda kalan bireylerin korkuyu nasıl yorumladığını ve nasıl tepki verdiklerini araştırmıştır. KMT'yi caydırıcılık teorisiyle birleştirerek bir model geliştirilmiştir. Bu model 559 çalışanla test edilmiş ve araştırmada, yanıt yeterliliğinin, tehdit ciddiyeti ve öz yeterliliğin önemli faktörler olduğu bulunmuştur. Ayrıca, yaptırım hızı, yaptırım ciddiyeti ve yaptırım kesinliğinin bilgi güvenliği politikalarına uyum niyeti üzerinde etkisinin olmadığı tespit edilmiştir.

Dang-Pham ve Pittayachawan (2015), kullanıcıların kötü amaçlı yazılımlardan kaçınma niyetini etkileyen faktörleri araştırmışlardır. Bu çalışma örnekleme 252 öğrenciden oluşturmaktadır. Öğrenciler, e-postalarını hem evde hem de üniversitede kontrol ederken aynı güvenli davranışları sergilemektedir. Kötü amaçlı web sitelerinden kaçınma ve

cihazlarını kilitleme konusunda, öğrencilerin evde kötü amaçlı URL'leri tespit etmeye daha istekli olduğu ve cihazlarını üniversitede daha fazla kilitlemeyi tercih ettikleri ortaya çıkmıştır

Hanus ve Wu (2016) bilgi güvenliği farkındalığının masaüstü güvenlik davranışı üzerindeki etkisini incelemek için koruma motivasyonu teorisini kullanmıştır. Örneklem olarak ABD' deki bir üniversitenin işletme fakültesi öğrencileri seçilmiştir. Araştırma sonuçlarına göre, yanıt yeterliliğinin ve öz yeterliliğin güvenlik davranışının önemli yordayıcıları olduğu ortaya çıkmıştır. Ancak, tehdit değerlendirmesinin ve yanıt maliyetinin masaüstü güvenlik davranışı üzerinde anlamlı bir etkisi olmadığı belirlenmiştir. Yani algılanan önem ve algılanan duyarlılık - güvenlik açığı masaüstü güvenlik davranışı üzerinde anlamlı bir etkiye sahip değildir. Benzer şekilde, yanıt maliyetinin de masaüstü güvenlik davranışı üzerinde anlamlı bir etkisi bulunamamıştır.

Menard vd. (2017), koruma motivasyon teorisi ile öz belirleme teorisini birleştirerek çalışanların siber güvenlik ile ilgili davranışsal niyeti ölçmüştür. Siber güvenlik davranışsal niyet üzerinde sadece yanıt yeterliliğinin anlamsız etkisi bulunmuştur. Algılanan tehdit öneminin, tehdit duyarlılığının, öz yeterliliğin ve tepki maliyetinin güvenlik davranışları üzerinde etkisi bulunmuştur.

Blythe ve Coventry (2018), kötü amaçlı yazılımdan korunma, yazılım güncelleme ve e-posta güvenliği davranışlarını yanıt yeterliliği, yanıt maliyeti ve öz yeterlilik faktörleri ile araştırmıştır. Çalışma örneklemini 526 çalışan oluşturmaktadır. Öz yeterlilik, kötü amaçlı yazılımdan koruma ve e-posta güvenliği davranışı için en güçlü belirleyici olduğu bulunmuştur.

Hooper ve Blunt (2019), BT çalışanlarının bilgi güvenliği davranışsal niyetlerini hangi faktörlerin etkilediğini belirlemek için koruma motivasyonu teorisi, caydırıcılık teorisine ve mantıklı eylem teorisine dayalı bir model geliştirmiştir. Çalışmanın sonuçlarına göre, yanıt maliyetlerinin ve yanıt yeterliliğinin davranışsal niyet üzerinde bir etkisinin olmadığı görülmüştür. Öz yeterliliğin niyet üzerinde ise önemli bir etkisinin olduğu belirlenmiştir.

Shahbaznezhad vd. (2021), kullanıcıların kimlik avı e-postalarına tıklamasını etkileyen faktörleri belirlemeyi araştırmıştır. Çalışma, kullanıcıların kimlik avı e-postalarını tıklama niyeti üzerindeki bireysel, organizasyonel ve teknolojik faktörlerden oluşan üç ana sınıfı incelemiştir. Çalışma sonuçlarına göre, destekleyici teknolojinin, çalışanların

kimlik avı e-postalarını ele alma davranışlarını açıklamada önemli bir rol oynadığı bulunmuştur.

Sulaiman vd. (2022), çalışanların siber güvenlik davranışının belirleyicilerini anlamak için koruma motivasyon teorisi kullanılmıştır. Çalışma, bir siber saldırı tespit edildiğinde kullanıcı farkındalığı ve tehdit değerlendirmesi ile kullanıcının başa çıkma değerlendirmesini etkilemede alışkanlığın etkisi arasında bir bağlantı kurmayı araştırmıştır. Bulgular, algılanan güvenlik açığı veya algılanan duyarlılık dışında tüm KMT faktörlerinin siber güvenlik davranışını önemli ölçüde etkilediğini göstermiştir.

Al-Shanfari vd. (2022), kamu sektörü çalışanlarının bilgi güvenliği farkındalığını değerlendirmek için Koruma Motivasyonu Teorisi, Planlı Davranış Teorisi, Genel Caydırıcılık Teorisi'ne dayanan kapsamlı bir teorik model geliştirilmiştir. Bu çalışma, bilgi güvenliği davranışının benimsenmesi ve bilgi güvenliği ihlali riskinin azaltılması için tahmin, kontrol, motivasyon, caydırıcılık, teknik bağlantılı ve kolaylaştırıcı koşullar gibi faktörleri inceleyerek kamu kurumlarının insan bileşenini nasıl yönetebileceklerini ve bilgi güvenliği farkındalıklarını nasıl artırabileceklerini açıklamaktadır. Araştırma, algılanan yaptırım kesinliği dışında, kullanılan faktörlerin bilgi güvenliği davranışının benimsenmesiyle pozitif yönde ilişkili olduğunu ortaya koymuştur

Khan vd. (2023), siber güvenlik eğitiminin siber güvenlik davranışsal niyeti üzerindeki etkisini araştırmıştır. Bu çalışmada lisans öğrencilerinin siber güvenlik bilgilerini artırmak için koruma motivasyon teorisine dayalı eğitimden yararlanılmıştır. Araştırma, öğrencilerin kendilerine yönelik tehditler ve karşı önlemler hakkındaki bilgilerinin önemli ölçüde arttığını ortaya koymaktadır. Öz yeterliliğin güvenlik niyetleri üzerinde pozitif anlamlı bir etkiye sahip olduğu ve hem ön hem de son test sonuçlarında en güçlü yordayıcı olduğunu vurgulamaktadır. Ancak, hem ön hem de son testlerde, bazı hipotezlerin (algılanan önem, algılanan duyarlılık, yanıt yeterliliği, yanıt maliyeti) bu çalışmada desteklenmediği bulunmuştur.

Bu makaleler KMT'nin siber güvenlik literatüründe merkezi bir rol oynadığını doğrulamaktadır.

Tablo 1*Literatür İncelemesi*

Yazar	Model	Uygulama Grubu	Değişkenler
Gurung vd. (2009)	KMT	232 Öğrenci	Algılanan Güvenlik Açığı, Algılanan Önem, Yanıt Yeterliliği, Yanıt Maliyeti, Öz Yeterlilik, Casus Yazılım Önleme Kullanımı
Ifinedo (2012)	KMT+ PDT	124 BT Çalışanı ve İşletme Yöneticisi	Algılanan Güvenlik Açığı, Algılanan Önem, Yanıt Yeterliliği, Yanıt Maliyeti, Öz Yeterlilik, Öznel Normlar, Bilgi Sistemleri Güvenlik Politikasına Tutum, Bilgi Sistemleri Güvenlik Politikasına Davranışsal Uyum Niyeti
Yoon vd. (2012)	KMT+ Alışkanlıklar Teorisi	202 Öğrenci	Algılanan Güvenlik Açığı, Algılanan Önem, Yanıt Yeterliliği, Yanıt Maliyetleri, Öz Yeterlilik, Öznel Norm, Güvenlik Alışkanlıkları, Davranışsal Niyet
Siponen vd. (2014)	KMT+ MET+ BDT	669 Çalışan	Şiddet, Güvenlik Açığı, Yanıt Yeterliliği, Öz Yeterlilik, Davranış, Normatif İnançlar, Ödüller, Kimlik Avı E-Postalarına Tıklamaya Yönelik Niyet
Crossler ve Bélanger (2014)	KMT	279 Katılımcı	Algılanan Güvenlik Açığı, Algılanan Önem, Öz Yeterlilik, Yanıt Yeterliliği, Yanıt Maliyetleri, Birleştirilmiş Güvenlik Uygulamaları
Johnston vd. (2015)	KMT+ GCT	559 Çalışan	Tehdit Önemi, Tehdit Duyarlılığı, Öz Yeterlilik, Yanıt Yeterliliği, Resmi Yaptırım Şiddeti, Gayri Resmi Yaptırım Şiddeti, Resmi Yaptırım Kesinliği, Gayri Resmi Yaptırım Kesinliği, Yaptırım Hızı, Uyum Niyeti
Boehmera vd. (2015)	KMT	565 +206 Öğrenci	Dolandırıcılığa Duyarlılık, Virüse Karşı Duyarlılık, Gizlilik Duyarlılığı, Dolandırıcılık Tehdidi Ciddiyeti, Virüs Tehdidi Ciddiyeti, Gizlilik Tehdidi Ciddiyeti, Gelişmiş Korumayla Başa Çıkma Yeterliliği, Yazılım Korumasıyla Başa Çıkma Yeterliliği, İletişimle Başa Çıkma Yeterliliği, Gelişmiş Yanıt Yeterliliği, Yazılım Yanıt Yeterliliği, Yanıt Maliyetler, Ödüller, Kişisel Sorumluluk, Güvenli Çevrimiçi Davranış
Safa vd. (2015)	KMT + PDT	212 BT Çalışanı	Tutum, Öznel Normlar, Algılanan Davranışsal Kontrol, Tehdit Değerlendirmesi, Öz Yeterlilik, Bilgi Güvenliği Bilinçli Bakım Davranışı
Pham ve Pittayachawan (2015)	KMT	252 Öğrenci	Güvenlik Açığı, Ciddiyet, Ödüller, Yanıt Yeterliliği, Yanıt Maliyeti, Öz Yeterlilik, Kötü Amaçlı Yazılımdan Kaçınma Davranışlarını Gerçekleştirme Niyeti

Tablolar Devamı

Hanus ve Wu (2016)	KMT	241 Öğrenci	Algılanan Önem, Algılanan Güvenlik Açığı, Öz Yeterlilik, Yanıt Yeterliliği, Yanıt Maliyeti, Masaüstü Güvenlik Davranışı
Aurigemma vd. (2016)	KMT	372 Öğrenci	Algılanan Tehdit Duyarlılığı, Algılanan Tehdit Önemi, Uyumsuz Ödüller, Korku, Yanıt Maliyetleri, Öz Yeterlilik, Yanıt Yeterliliği, Koruyucu Yanıt, Koruma Motivasyonu Niyetleri
Chou ve Chou (2016)	KMT	505 Öğretmen	Algılanan Güvenlik Açığı, Algılanan Önem, Öz Yeterlilik, Yanıt Yeterliliği, Yanıt Maliyetleri, Infosec Davranışı
Warkentin vd. (2016)	KMT	253 Öğrenci	Algılanan Tehdit Şiddeti, Algılanan Tehdit Duyarlılığı, Tepki Etkinliği, Öz Yeterlilik, Algılanan Dış Koşullar, Devam Niyeti
Thompson vd. (2017)	KMT	629 Kullanıcı	Önceki Deneyim, Algılanan Duyarlılık, Algılanan Önem, Öz Yeterlilik, Yanıt Yeterliliği, Yanıt Maliyeti, Öznel Norm, Tanımlayıcı Norm, Psikolojik Sahiplenme, Güvenlik Niyetleri
Wang vd. (2017)	KMT	547 Kullanıcı	Algılanan Kimlik Avı Duyarlılığı, Algılanan Kimlik Avı Şiddeti, Algılanan Kimlik Avı Tehdidi, Algılanan Tespit Etkinliği, Pishing Kaygısı, Başa Çıkma Uyumluluğu, Tespit Çabası, Kaçınma, Duygu Odaklı Başa Çıkma, Tespit Doğruluğu
Bélangera vd. (2017)	KMT + PDT	535 Katılımcı	Organizasyonel Tetikleyiciler, Güvenlik Politikası Farkındalığı, Tutum, Öznel Norm, Öz Yeterlilik, Algılanan Tehdit Şiddeti, Algılanan Tehdit Savunmasızlığı, Erken Uyum Davranışı, Erken Uyum Niyeti
Geil vd. (2017)	KMT + HBM	138 Çalışan	Algılanan Duyarlılık, Algılanan Önem, Algılanan fayda, Öz Yeterlilik, Eyleme geçme çağrısı, Siber Güvenlik Davranışı
Blythe ve Coventry (2018)	KMT	526 Çalışan	Deneyim, Şiddet, Duyarlılık, Öz Yeterlilik, Yanıt Yeterliliği, Yanıt Maliyetleri, Sorumluluk, Psikolojik Sahiplenme, Niyet
Torten vd. (2018)	KMT	400 BT Çalışanı	Algılanan Önem, Algılanan Güvenlik Açığı, Öz Yeterlilik, Yanıt Yeterliliği, Yanıt Maliyeti, Masaüstü Güvenliği
Hanus vd. (2018)	KMT	172 Çalışan	Algılanan Maliyetler, Sorumluluk, Algılanan Etkililik, Öz Yeterlilik, Algılanan Duyarlılık, Algılanan Önem, Bilgi Güvenliği Politikası Farkındalığı, Önceki Deneyim, Bilgi Güvenliğine İlgili Duyma, Bilgi Güvenliği Politikalarına Uyum Konusunda Tutum, Bilgi Güvenliği Politikalarına Ve Güvenlik Bilincine Uyum Niyeti

Tablolar Devamı

Marett vd. (2019)	KMT	461 Öğrenci	Tehdit Şiddeti, Tehdit Zayıflığı, Genel Tehdit, Yanıt Yeterliliği, Öz Yeterlilik, Yanıt Maliyetleri, Genel Başa Çıkma, Davranışsal Niyet
Giwah vd. (2019)	KMT	390 Kullanıcı	Algılanan Tehdit Şiddeti, Algılanan Tehdit Duyarlılığı, Algılanan Yanıt Maliyeti, Yanıt Etkinliği, Mobil Öz Yeterlilik, Mobil Cihaz Güvenliği Kullanımı
Ameen vd. (2019)	KMT+ GCT	1156 Çalışan	Öz Yeterlilik, Algılanan Yaptırım Şiddeti, Algılanan Risk Hassasiyeti, Yanıt Maliyeti, Algılanan Yaptırım Kesinliği, Olumsuz Sonuçların Ciddiyeti, Tepki Etkinliği, Belirsizlikten Kaçınma, Güç Mesafesi, Bireycilik Vs Kolektivizm, Erkeklik Vs Kadınlık, Akıllı Telefon Güvenliğine Yönelik Davranışsal Niyet
Hooper ve Blunt (2019)	KMT + MET+ GCT	70 Çalışan	BT İpuçları, Olasılık, Etki, Yanıt Maliyeti, Yanıt Yeterliliği, Öz Yeterlilik, Yanıt Faydaları, Sosyal Normlar, Tespit, Yaptırım, Niyet
Rajab ve Eydgahi (2019)	KMT+ GCT+ PDT+ Organizasyonel Teori	206 Çalışan	Tutum, Özel Normlar, Algılanan Davranışsal Kontrol, Tehditlerin Algılanan Önemi, Algılanan Güvenlik Açığı, Yanıt Maliyeti, Yanıt Yeterliliği, Öz Yeterlilik, Yaptırımların Algılanan Önemi, Algılanan Tespit Kesinliği, Algılanan Hız, Akran Baskısı, Üst Yönetim Desteği, Örgütsel İklim, Bilgi Güvenliği Politikası Uyumluluğu
Li vd. (2019)	KMT	579 Çalışan	Akran Davranışı, Eylem İşareti, Algılanan Önem, Algılanan Güvenlik Açığı, Algılanan Engeller, Yanıt Yeterliliği, Öz Yeterlilik, Siber Güvenlik Koruma Davranışı
Crossler vd. (2019)	KMT	487 Öğrenci	Algılanan Önem, Algılanan Duyarlılık, Ödül, Öz-Yeterlik, Yanıt Yeterliliği, Yanıt Maliyetleri, Davranışsal Niyet
Gillam ve Foster (2020)	KMT + TTKT	184 Çalışan	Algılanan Duyarlılık, Algılanan Güvenlik, Algılanan Etkinlik, Algılanan Maliyet, Öz Yeterlilik, Kaçınma Motivasyonu, Kaçınma Davranışı, Riskli Siber Güvenlik Davranışı
Gillam ve Waite (2021)	KMT	206 Çalışan	Algılanan Duyarlılık, Algılanan Önem, Öz Yeterlilik, Algılanan Yeterlik, Algılanan Maliyet, Kaçınma Motivasyonu, Kaçınma Davranışı
Li vd. (2022)	KMT	224 Çalışan	Algılanan Önem, Algılanan Güvenlik Açığı, Ödül, Öz Yeterlilik, Yanıt Yeterliliği, Yanıt Maliyetleri, Bilgi Güvenliği Sistemine Uyum Niyeti

Tablolar Devamı

Nehme ve George (2022)	KMT	498 Kullanıcı	Kendini Geliştirme, Tehdit Güvenlik Açığı, Tehdit Şiddeti, Öz Yeterlilik, Yanıt Yeterliliği, Yanıt maliyetleri, Korku, Umut, Koruma Motivasyonu
Sulaiman vd. (2022)	KMT	446 Çalışan	Algılanan Güvenlik Açığı, Algılanan Önem, Algılanan Engel, Güvenlik Yanıt Yeterliliği, Yanıt Öz Yeterliliği, Siber Güvenlik Davranışı
Bhadauria ve Chennamani (2022)	KMT+ Theory of Self Regulation	315 Katılımcı	Öz Yeterlilik, Yanıt Yeterliliği, Özel Norm, Kişisel Yenilikçilik, Davranışsal Niyet
Al-Shanfari vd. (2022)	KMT+ GCT+P DT	391 Çalışan	InfoSec Tutumu Özel Normlar, Algılanan Davranışsal Kontrol, Yanıt Yeterliliği, Algılanan Tehdit Savunmasızlığı, Algılanan Yaptırımların Kesinliği, Algılanan Yaptırımların Şiddeti, Organizasyonel Destek, InfoSec İletişim Kanalları, Güvenlik Eğitimi, Eğitim ve Farkındalık, Davranışsal Niyet
Li vd. (2022)	KMT	387 Çalışan	Algılanan Siber Güvenlik Önemi, Siber Saldırlarda Algılanan Güvenlik Açığı, Yanıt Yeterliliği, Öz Yeterlilik, Yanıt Maliyeti, Güvenliği Koruma Motivasyonel Davranış
Sharma ve Aparicio (2022)	KMT	341 Çalışan BT	Tehdit Şiddeti, Tehdit Güvenlik Açığı, Yanıt Yeterliliği, Yanıt Maliyeti, Öz Yeterlilik, Bilgiyi Korumaya Yönelik Davranışsal Niyet
Aigbefo vd. (2022)	KMT + PDT	294 Çalışan	Özel Norm, Tutum, Dayanıklılık, Alışkanlık, Algılanan Önem, Algılanan Duyarlılık, Uyum Niyeti
Al-Kumaim ve Alshamsi (2023)	KMT	310 Çalışan	Algılanan Güvenlik Açığı, Algılanan Önem, Yanıt Yeterliliği, Öz Yeterlilik, Yanıt Maliyetleri, Hükümetin Uyarıda Bulunması, Siber Saldırıların Önleme
Khan vd. (2023)	KMT	154 Öğrenci	Algılanan Önem, Algılanan Güvenlik Açığı, Öz Yeterlilik, Yanıt Yeterliliği Etkinliği, Yanıt Maliyetleri, Tehdit Bilgisi, Karşı Tedbir Bilgisi, Algılama, Siber Güvenlik Davranışsal Niyetleri
Alraja vd. (2023)	KMT + Alışkanlıklar Teorisi	348 Çalışan	Yanıt Yeterliliği, Tehdit, Alışkanlık, Rol Değerleri, Korku, Nötralizasyon, Tepki, Niyet

BÖLÜM 3. ARAŞTIRMA YÖNTEMİ

Bu bölümde, temel araştırma problemi ve alt araştırma problemleri sunulduktan sonra araştırma tasarımları incelenmiştir. Bu teze uygun araştırma paradigması ve nedenleri tartışılmıştır. Sonrasında anakütle ve örneklem, veri toplama yöntemleri ve araştırma enstrümanının geliştirilmesi adımları açıklanmıştır.

3.1. Araştırma Problemi

Dijital çağda bilgisayar sistemleri, internet ve akıllı cihazlar gibi teknolojiler toplumların günlük yaşamında temel bir rol oynamaktadır. Yeni teknolojilerin kolaylık ve verimliliğinin tadını çıkarırken, her geçen gün teknoloji kullanımından kaynaklanan yeni riskler ve tehditlerle de karşı karşıya kalmaktayız. Diğer taraftan uzaktan çalışmanın, sanal konferansların ve dijital cihazlara olan bağımlılığın arttığı bir ortamda siber saldırıların sıklığı, hacmi ve karmaşıklığı da artmaktadır (L. Li vd., 2022; Lu ve Xu, 2019).

Son yıllarda, değerli verilerin kasıtlı ve kasıtsız olarak sızdırılması ve çalınması gibi birçok tehdit vakaları rapor edilmiştir. IBM Security (2020) raporuna göre, önemli siber güvenlik ihlallerinin yaklaşık %36'sı şirket içi kişilerin veya çalışanların uyumsuz davranışlarından, uzaktan çalışmadan ve güvenlik becerisi eksikliklerinden kaynaklanmaktadır (L. Li vd., 2022).

Küresel olarak, tüm kurumların %72,7'si 2023 yılında bir fidye yazılımı saldırısı yaşamıştır (Statista, 2024b). 2023'ün 2. çeyreğinde dünya genelinde haftalık siber saldırılarda %8'lik bir artış yaşanarak, kurumlar haftada ortalama 1.258 saldırıyla karşı karşıya kalmıştır (Check Point, 2023). Başka bir rapora göre ise siber suç maliyetlerinin 2025 yılına kadar 10,5 trilyon dolara ulaşması beklenmektedir (Cobalt, 2024).

İşletmeler özelinde örnek vermek gerekirse, bulut hizmeti sağlayıcısı Tietoevry'nin İsveç'teki veri merkezleri bir fidye yazılımı saldırısına maruz kalmıştır ve bu sebeple ülke genelinde birçok işletme e-ticaret faaliyetlerini yürütemediği için kapanmak zorunda kalmıştır (Petkauskas, 2024). Benzer şekilde, havacılık ve uzay bileşenleri üretim lideri Airbus, Türk Hava Yolları çalışanının crack'li bir uygulama indirmesi ve kurması üzerine siber saldırıya maruz kalmıştır (Pandagle, 2023b). Çalışanın dikkatsizliği nedeniyle Airbus firması bilgisayar korsanlarının hedefi haline gelmiş ve güvenlik ihlali yaşamıştır

Rhee vd. (2009) siber güvenlik risklerinin önlenmesi ve azaltılması kısaca yönetiminin iki aşamalı olduğunu ileri sürmüştür: 1) açılır pencere engelleme, casus yazılım önleme ve virüsten koruma yazılımı gibi güvenlik yazılımı ve özellikleri; 2) bilgisayar ve internet kullanımına ilişkin güvenlik üzerine odaklanmış bilinçli davranış. Buradan hareketle sadece bir güvenlik yazılımı satın almakla veya güvenlik duvarını aktif hale getirmek güvenlik için yeterli olmamaktadır. Son kullanıcılara bilgi ve bilgisayar güvenliği konusunda farkındalık kazandırmak ve söz konusu bu alanda eğitimlerin verilmesi gerekmektedir. Kurumların siber güvenlik üzerine eğitim, öğretim ve farkındalık programlarını uygulamadan önce çalışanların neyin motive ettiğini hangi faktörlerin güvenlik davranışı gerçekleştirmede etkili olduğunu araştırması ve belirlemesi gerekmektedir.

Bilgisayar korsanları bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini kendi çıkarları doğrultusunda değiştirmek için farklı yöntemler kullanırken, çalışanlar ise kasıtlı olarak veya ihmal yoluyla bilgi güvenliği açısından büyük bir tehdit oluşturmaktadır. Hesap bilgilerini paylaşmak, internetten herhangi bir yazılım indirmek, şifreleri yapışkan kâğıda yazmak, TC kimlik numaralarını kullanıcı adı veya şifre olarak kullanmak yaptıkları hatalara örnektir. Çalışanların ihmali, bilgisizliği, bilinçsizliği, ilgisizliği ve dirençleri genellikle güvenlik ihlallerinin temel nedenleridir. Çalışanların zayıf bilgi güvenliği davranışları bu alandaki temel sorundur. Bu sorunun giderilmesine yönelik literatürde bazı çalışmalar mevcuttur fakat bu çabalar uzaktan veya hibrit şeklinde çalışanlar için yetersiz veya sınırlı olduğundan sunulan modelin, çalışanların davranışlarına dayalı siber güvenlik olayları riskini azaltmada kurumlara yol gösterici bir rehber olacağı düşünülmektedir.

Çalışma, çalışanların kendilerini ve organizasyonlarını siber saldırılardan korumaya yönelik davranışlarını etkileyen faktörlere odaklanmıştır. Bu doğrultuda araştırma kapsamında ele alınacak temel araştırma problemi “Koruma motivasyon teorisi faktörleri, mantıklı eylem teorisi faktörleri ve alışkanlıklar teorisi faktörleri bilişim sektöründe uzaktan veya hibrit çalışanların siber hijyen davranışlarını nasıl etkiler? olarak belirlenmiştir. Bu temel araştırma problemini cevaplamak adına aşağıdaki alt sorulara cevap aranacaktır.

- 1) Koruma motivasyon teorisi faktörleri BT çalışanlarının siber hijyenini nasıl etkiler?
- 2) BT çalışanlarının güvenlik alışkanlıkları siber hijyeni nasıl etkilemektedir?

3) Çalışma tipine (uzaktan ve hibrit) göre BT çalışanlarının siber hijyenini etkileyen faktörler nasıl farklılık gösterir?

Temel araştırma problemi ve alt araştırma problemler dahilinde bu çalışmanın temel amacı, bilişim sektöründe uzaktan ve hibrit şekilde çalışanların siber hijyenini etkileyen faktörler üzerine güvenilir ve geçerli bir model geliştirmektir.

3.2. Araştırma Tasarımı

Farklı yazarlar araştırma tasarımına farklı anlamlar yüklemektedir. Bazıları araştırma tasarımının tamamen uygun yöntemin (nitel, nicel veya karma) seçilmesiyle ilgili olduğunu düşünmektedir. Bazı araştırmacılar ise araştırma boyunca doğru adımların izlenmesiyle ilgili olduğunu düşünmektedir (Saunders vd., 2012). Creswell'e (2014) göre araştırma tasarımı, araştırma sorusuna ve alt sorularına doğru cevapları bulmak için oluşturulan bir çerçevedir. Araştırma tasarımı, araştırma problemine özgü yöntem ve prosedürleri içermelidir. Araştırma tasarımının seçimi araştırma probleminin veya konunun doğasına, araştırmacıların araştırmacının kişisel deneyimlerine ve çalışmanın hedef kitlesine de dayanmaktadır (Creswell, 2014).

Creswell'e göre üç tür araştırma tasarım vardır: nitel, nicel ve karma yöntemler. Bu üç yaklaşım ilk başta göründükleri kadar birbirinden farklı değildir. Nitel ve nicel yaklaşımlar zıt kutuplar olarak görülmemelidir. Düz bir çizgi üzerindeki farklı uçları temsil etmektedir (Newman ve Benz, 1998). Bir çalışma nicel olmaktan ziyade nitel olma eğiliminde olabilir veya bunun tersi de geçerli olabilir. Karma yöntem araştırması hem nitel hem de nicel yaklaşımların unsurlarını içerdiği için bu çizginin tam ortasında yer almaktadır (Creswell, 2014).

Araştırmacıların çalışmaya getirdiği temel felsefi varsayımlar, araştırmada genel olarak kullanılan araştırma stratejisi türleri ve kullanılan belirli yöntemler konusunda nitel ve nicel araştırmalar farklılaşmaktadır. Nitel araştırmalarda, bireylerin veya grupların sosyal veya insani bir soruna atfettiği anlamı keşfetme ve anlama amacı vardır. Nicel araştırma, değişkenler arasındaki ilişkiyi inceleyerek nesnel teorileri test etme amacı vardır. Karma yöntem araştırmalarında, hem nitel hem de nicel biçimleri birleştiren veya ilişkilendiren bir araştırma yaklaşımı benimsenmektedir (Creswell, 2014). *Şekil 16*'da farklı seviyeler ait araştırma yaklaşımları sunulmuştur.

Şekil 16

Temel Araştırma Yaklaşımları

Paradigmal Seviye	
Yorumlayıcı Yaklaşım (Interpretive) Evrensel gerçeklik yoktur. Araştırmacının düşünce çerçevesinden anlama ve değerlendirme söz konusudur.	Pozitivist Yaklaşım (Positivist) Dünya önceden belirlenmiş neden-sonuç ilişkilerine uyumludur. Karmaşıklıkla indirgemecilik yoluyla başa çıkılabilir. Nesnellik, ölçme ve yinelenebilirlik vurgusu .
Ontolojik Seviye	
Görecilik (Relativism) Aklın öznel yorumları şeklinde birçok gerçeklik olduğuna inanmak. Sosyal olarak yayılan kavramlar gerçekliğin nasıl algılandığına yön verir ve bu durum farklı dil ve kültürlerle göre değişiklik gösterir.	Gerçekçilik (Realism) Varlığın, bireyin algısından bağımsız, katı ve somut şekilde önceden bulunan yapılardan oluştuğuna inanmak.
Epistemolojik Seviye	
Öznel (Subjectivist) Araştırmacı ile araştırmanın konumu arasındaki ayırım yıkılmıştır. Araştırma bulguları araştırmacı ile araştırma konumu arasındaki etkileşimden ortaya çıkar ve araştırmacının değerleri ve inançları temel araçlardır.	Nesnel (Objectivist) Araştırmacının araştırmanın konumundan bağımsız durmasının hem olası hem de zorunlu olması durumu. Araştırmacının doğru olmayan herhangi bir değer ya da önyargıya hakim olduğu durumda gerçeklik tarafsızca gözlemlenmelidir.
Metodolojik Seviye	
Kalitatif (Qualitative) Varlığın ne kadar olduğundan ziyade, hangi varlıkların mevcut olduğunu belirlemek. Yoğun tanım, daha az yapılandırılmış, ihtiyaçlara ve araştırma konumuna daha duyarlı.	Kantitatif (Quantitative) Olgular ve nedensellik ilişkilerinin matematiksel ve istatistiksel teknikleri kullanarak belirlemek. Örnekler daha büyük olabilir ve daha iyi temsil edebilir. Sonuçlar bilinen hata limitleri dahilinde daha büyük popülasyonlar için genelleştirilebilir.
Keşfedici (Exploratory) Araştırma verisindeki modelleri keşfetmek, onları açıklamak/anlamak ile ilgilenir. Temel tanımlayıcı yapılar söz konusudur. Hipotez oluşturmada yol göstericidir.	Doğrulamacı (Confirmatory) Hipotezlerin sınanması ve teoremin onaylanması ile ilgilenir. Araştırmanın pozitivist ve kantitatif yöntemlerini takip etmeye yatkındır.
Tümevarım (Induction) Kapsamlı bir genelleştirme için belirli örneklerden hareket eder. Yeni kanıtlar sonuçların revize edilmesine izin verir. Birçok felsefeci tarafından eleştirilse de, teori ve hipotez kavramlarında önemli rol oynar.	Tümdengelim (Deduction) Belirli örneklerle özellik atfetmek için genel sonuçları kullanır. Önerme doğruysa sonuçların yanlış olması mümkün değildir ki böyleyse iddia geçerlidir. Doğrulamacı/yanlışlama teorileri ve hipotez testleri ile ilişkilidir.
Etik ve Değerler Seviyesi (Axiological)	
Uygunluk (Relevance) Doğru araştırma sorusunun dışsal geçerliliği ve uygulama için uygunluğu, araştırılabilir olmasına rağmen odağı kısıtlayan “sıkı” yöntemlerden çok daha önemlidir.	Keskinlik (Rigour) Pozitivist paradigmaya uygun olarak, sıkı deneysel kontrol ve kantitatif teknikler aracılığıyla iç geçerliliği öne çıkaran kuramsal-tümdengelim sınaması karakteristik özelliğidir.

Kaynak:(Akbiyık, 2012)

Nicel bir yöntem, değişkenler arasındaki bağlantıyı istatistiksel bir yöntemle incelemeye yönelik bir süreci içerir (Dyer, 2006). Mevcut araştırma soruları, yordayıcı değişkenler ile bağımlı değişken arasındaki ilişkilerin kurulmasıyla ilgilidir.

Bu çalışmada nicel yöntem araştırma tasarımı uygun görülmüştür. Sebebi ise çalışma amacı yordayıcı değişkenler ile bağımlı değişkenler arasındaki ilişkileri incelemektir. Literatürde, uzaktan çalışanların siber hijyen davranışını motivasyonel faktörler ile

inceleyen ve faktörler arası ilişkileri destekleyecek ampirik veriler sınırlıdır (Ifinedo, 2012; Thompson vd., 2017b; Tsai vd., 2016).

3.3. Araştırma Modeli ve Hipotezleri

Bu araştırma, bilişim sektöründe çalışanların siber hijyen davranışını etkileyen faktörleri incelemeyi amaçlamaktadır. Araştırmacının amacı doğrultusunda oluşturulan teorik model ve hipotezler detaylı olarak sunulmaktadır.

İlk olarak, algılanan güvenlik açığı, bireyin tehdit edici olayların olasılığına ilişkin değerlendirmesidir (Ifinedo, 2012). Başka bir tanıma göre ise kullanıcıların bir güvenlik tehdidinin meydana gelmesine ilişkin subjektif olarak tahmin etme olasılığını ifade eder (Thompson vd., 2017). Özetle kullanıcının kişisel veya iş bilgisayarına ve bilgilerine yönelik güvenlik tehditleriyle karşılaşacağına ne ölçüde inandığı olarak tanımlanmaktadır. Algılanan güvenlik açığının genellikle kurumsal alandaki güvenlik davranışını etkilediği bulunmuştur (Ifinedo, 2012; M. Siponen vd., 2014; Workman vd., 2008). Örneğin bazı araştırmalarda algılanan güvenlik açığının güvenlik davranışı üzerinde olumlu etkisi bulunmuşken (Claar ve Johnson, 2012; Liang ve Xue, 2010a), bazı araştırmalarda beklenmedik bir şekilde güvenlik davranışı üzerinde olumsuz bir etkiye sahip olduğunu bulunmuştur (R. Crossler ve Bélanger, 2014; R. E. Crossler, 2010; N. F. Khan vd., 2023). Bazı araştırmalarda ise algılanan güvenlik açığının güvenlik davranışı üzerinde hiçbir etkisinin olmadığı bulunmuştur (Blythe ve Coventry, 2018; Hanus ve Wu, 2016; Sulaiman vd., 2022; Tsai vd., 2016; Yoon vd., 2012). Literatürdeki bu karışık bulgulara rağmen, bu çalışmada Rogers (1983) tarafından önerilen ilişkiyle tutarlı olarak aşağıdaki hipotez önerilmiştir.

H1: Algılanan güvenlik açığı, BT çalışanların siber hijyen davranışsal niyetini olumlu yönde etkileyecektir.

Genel olarak bireyler güvenlikle ilgili bir tehdit algıladıklarında risk miktarına göre davranışlarını değiştirmektedirler (Milne vd., 2000; Workman vd., 2008). Algılanan önem, bir tehdidin ortaya çıkışının yol açabileceği zararın ne kadar ciddiye alındığını ifade etmektedir (Johnston ve Warkentin, 2010). Tehdidin ortaya çıkışının ve gerçekleşmesinin olası etkileri anlamak olarak da tanımlanmaktadır (Mou vd., 2018). Ifinedo (2012) algılanan önemi, kullanıcıların kişisel bilgisayarlarına yönelik tehditlerin sonuçlarının zararlı olacağına ne ölçüde inandıkları olarak tanımlamaktadır. Bireyin güvenlik tehditlerine karşı zafiyet algısı yüksekse ve bu tehditlerin etkilerinin yüksek

olduğunu düşünüyorsa siber güvenlik uygulamalarının benimsenmesi kuvvetle muhtemeldir (Khan vd., 2023).

Çalışanlar kurumun bilgi sistemleri varlıklarına yönelik bir güvenlik tehdidi algılayarsa, bu çalışanların bilgi güvenliği politikalarında belirtilen yönergeleri ve gereklilikleri takip etmesi daha olasıdır (Bulgurcu vd., 2010; M. Siponen vd., 2007). Öte yandan, eğer bir çalışan kurumsal bilgi sistemleri varlıkları konusunda bir güvenlik tehdidi algılamazsa, bilgi güvenliği politikalarına uymayabilir özetle güvenlik davranışlarını gerçekleştirmeyebilir. Bu nedenle, bireyin algılanan önemi, güvenlik eylemlerini takip etme niyetleriyle pozitif olarak bağlantılı olma eğilimindedir (Pechmann vd., 2003).

Literatürde algılanan önemin siber güvenlik davranışları üzerindeki etkisini bildiren birçok çalışma vardır (Bulgurcu vd., 2010; Burns vd., 2017; Posey vd., 2016). Marett vd. (2011) tarafından yapılan bir çalışmada, algılanan önemin güvenlik davranışı üzerinde olumlu bir etkisi olduğu bulunmuştur. Benzer şekilde, başka bir araştırmada algılanan önemin web sayfalarıyla ilgili güvenli davranışları üzerinde güçlü bir etkisi olduğu bulunmuştur (Abraham ve Chengalur-Smith, 2019). Herath ve Rao (2009a) tarafından yapılan çalışmada, algılanan önemin çalışanların bilgi sistemleri güvenlik politikalarını benimseme niyeti üzerinde anlamlı bir etkiye sahip olduğunu bulunmuştur.

Woon vd. (2005), bilgisayar kullanıcılarının, evlerindeki kablosuz ağdaki bir ihlalin zararlı olacağına inanmaları durumunda kablosuz güvenlik önlemlerini etkinleştirme olasılıklarının daha yüksek olduğunu bulmuştur. Fakat Zhang ve McDowell (2009) tarafından yapılan çalışmada algılanan önemin, şifre güvenliği davranışı üzerinde bir etkisinin olmadığını bulunmuştur. Tsai vd.. (2016) tarafından yapılan araştırmada ise algılanan önemin bilgisayar kullanıcılarının güvenlik niyetleri üzerinde olumsuz bir etkiye sahip olduğunu bulunmuştur. Bu araştırmada ise Rogers (1983) tarafından önerilen ilişkiyle tutarlı olarak çalışanların, güvenlik tehditlerin önemli olacağına inanmaları durumunda bilgisayarlarında koruyucu güvenlik önlemlerini alma niyetinde olma olasılıklarının daha yüksek olacağı önerilmektedir.

H2: Algılanan önem, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyecektir.

Koruma motivasyon teorisinin bir diğer bileşeni başa çıkma değerlendirmesi siber güvenlik davranışlarını yönlendirme de etkilidir (Doane vd., 2016). Başa çıkma değerlendirmesi genellikle siber güvenlik davranışlarını olumlu yönde etkilemede çok

daha net bir rol oynamaktadır (Ifinedo, 2012). Başa çıkma değerlendirmesi yanıt maliyeti, yanıt yeterliliği ve öz yeterlilik olmak üzere üç faktörden oluşmaktadır. İlk faktör yanıt maliyeti, bireyin koruyucu davranışlarla ilgili maliyetler hakkındaki algısıdır (Mou vd., 2022). Yanıt maliyetleri yalnızca finansal maliyeti değil, aynı zamanda kullanıcının koruyucu davranışla ilişkilendirebileceği herhangi bir zamanı, çabayı veya rahatsızlığı da ifade etmektedir (Pahnila vd., 2007). Bireyler bilgi varlıklarının algılanan iş değerinden veya öneminden bağımsız olarak, bilgi güvenliği önlemleri hakkında farklı maliyet-fayda tutumlarına sahiptirler (Workman vd., 2008). Bu maliyetler genellikle davranışsal motivasyonu azaltır çünkü birey bir eyleme geçmeden önce bir tür maliyet-fayda analizi yapabilmektedir. Bu nedenle bireyler, bir önlem için önemli miktarda kaynağın (zaman, çaba ve para) harcanacağını algılayarsa, önerilen yanıtları takip etme veya benimseme konusunda çekimser davranmaktadır (Milne vd., 2000). Eğer bir önlemin uygulanması için az miktarda kaynağa ihtiyaç duyulursa bu önlemi benimseme ihtimali yüksek olmaktadır (Pechmann vd., 2003; Workman vd., 2008). Yanıt maliyetinin azaltılması, bireyin önerilen davranışı gerçekleştirme olasılığını artırma eğilimindedir (Woon vd., 2005). Başka bir ifadeyle siber güvenlik davranışıyla ilgili çaba, zaman ve para maliyetleri çok yüksekse, bireylerin siber güvenlik davranışını gerçekleştirme olasılığı daha düşüktür.

Yanıt maliyeti kişisel siber güvenlik davranışlarını benimseme de önemli bir rol oynamaktadır. Bazı araştırmalarda yanıt maliyetinin siber güvenlik davranışları gerçekleştirme niyetleri üzerindeki olumsuz etkisi bulunmuştur (Liang ve Xue, 2010b; Mou vd., 2022; Woon vd., 2005). Ifinedo (2012) araştırmasında yanıt maliyetinin bilgi güvenliği sistemleri politikasına uyum niyetleri etkilemediğini tespit etmiştir. Benzer şekilde Crossler ve Bélanger (2014) araştırmasında yanıt maliyetinin güvenlik pratikleri ile anlamlı bir ilişkisinin olmadığı tespit etmiştir. Van Hooper ve Blunt (2019), BT çalışanlarının bilgi güvenliği davranışsal niyetlerini araştırdığı çalışmada, yanıt maliyetlerinin niyet üzerinde önemli bir etkisinin olmadığı görülmüştür. Bu doğrultuda çalışmanın hipotezi aşağıdaki gibi önerilmiştir.

H3: Yanıt maliyeti, BT çalışanlarının siber hijyen davranışsal niyetini olumsuz yönde etkileyecektir.

Baş çıkma değerlendirmesinin diğer iki faktörü, yanıt yeterliliği ve öz yeterlilikte siber güvenlik davranışlarının yönlendirmede etkilidir (Doane vd., 2016). Öz-yeterlik, bireyin koruyucu davranışı yeterli bir şekilde yerine getirme konusundaki algılanan yeteneğidir.

Yani kişinin istenen sonuçları elde etmek için gereken davranışı başarıyla yerine getirebileceğine dair olan inancıdır (Bandura, 1977). Yanıt yeterliliği ise , tehdidin engellenmesinde koruyucu davranışın algılanan yeterliliğidir (Posey vd., 2016). Başka bir ifadeyle yanıt yeterliliği, bireyin koruyucu bir davranışın algılanan tehdidi azaltmada yeterli olup olmadığına dair inancı olarak tanımlanmaktadır (Burns vd., 2017).

BT çalışanlarının bilgi güvenliği davranışı bağlamında öz yeterlilik, bireyin bir bilgi güvenliği kontrolünü uygulamak için gerekli eğitime ve/veya deneyime sahip olduklarına, istenen davranışı gerçekleştirme konusunda yetkin olduklarına veya bunu anladıklarına olan inancı ifade eder. BT çalışanlarının bilgi güvenliği davranışı bağlamında yanıt etkinliği ise, bireyin istenen davranışın bir riskin ortaya çıkma olasılığını ve/veya etkisini azaltmada pratik, verimli ve etkili olduğuna dair güvenini ifade eder. Yanıt yeterliliğinin, çalışanların güvenlik politikasına uyma veya tavsiye edilen güvenlik davranışlarını takip etme niyetleri üzerinde olumlu bir etkiye sahip olduğu bulunmuştur (Bulgurcu vd., 2010; Ifinedo, 2012; Vance vd., 2012; Workman vd., 2008).

Literatürde öz yeterlilik ve yanıt yeterliliği ile koruyucu güvenlik davranışı gerçekleştirme niyeti arasında pozitif ilişkiler olduğunu gösteren çok sayıda çalışma bulunmaktadır (Abraham ve Chengalur-Smith, 2019; Bulgurcu vd., 2010; Ifinedo, 2012; Vance vd., 2012). Literatürdeki bu görüşlere uygun olarak, hipotez aşağıdaki şekilde ifade edilebilir:

H4: Yanıt yeterliliği, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyecektir.

H5: Öz yeterlilik, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyecektir.

Öznel normlar, başkalarına danışılarak veya başkalarının davranışları gözlemlenerek bilgi verilen, belirli bir eyleme uymaya yönelik normatif uyarıcılar, inançlar ve motivasyonlardır (Ajzen, 1991). Cheng vd. (2013) göre öznel normlar, bireyin kendisi için önemli olan kişilerin belirli bir davranış hakkında ne düşündüğüne ilişkin algısı olarak tanımlanmaktadır. Bireysel davranışların, çevredeki norm olarak gözlemlenen şeylerden etkilendiği veya motive edildiği savunulmaktadır (Johnston ve Warkentin, 2010). Bazı çalışmalarda öznel norm KMT modeline dahil edilmiş ve bilgisayar güvenliği ile ilgili politika veya yazılımın benimsenmesinin önemli bir yordayıcısı olduğu bulunmuştur (Herath ve Rao, 2009a; Ifinedo, 2012; Lee ve Larsen, 2009).

Kurumlardaki bilişim sistemleri güvenliği politikaları uyumluluğu bağlamında, çalışanların, üstlerinin, iş arkadaşlarının ve astlarının bu tür yönergelere uyduğunu ve uyduğunu fark etmeleri halinde, büyük olasılıkla kurumların güvenlik politikalarına uymaları muhtemel olduğu savunulmaktadır (Chan vd., 2005). Bazı çalışmalarda öznel normların organizasyonlarda bilişim sistemleri güvenliği politikaları uyumluluğunu önemli ölçüde etkilediği bulunmuştur (Bulgurcu vd., 2010; Herath ve Rao, 2009a; Lee ve Larsen, 2009).

Öznel normlar örgüt üyeleri üzerinde belirli bir davranışı gerçekleştirme veya yapmaktan kaçınma yönündeki sosyal baskıyı gösterirler. BT organizasyonlarında sosyal çevre baskısı, siber güvenlik farkındalığını artırarak ve veri ihlali gibi tehditleri azaltarak etkili ve önemli bir rol oynamaktadır (Cheng vd., 2013). Çin'deki BT organizasyonlarında BT uzmanı olarak çalışanlar üzerinden bilgi güvenliği davranışının araştırıldığı bir çalışmada öznel normların güvenlik davranışı üzerinde anlamlı etkisi olduğu bulunmuştur (Ma, 2022). Bu çalışma sonuçlarına göre, öznel normların bir BT uzmanının tehditler (örn. Bilgi güvenliği ihlali sorunları) karşısında bilgi güvenliğini koruyucu davranışları kolaylaştırmada önemli rol oynadığını göstermektedir. Söz konusu bu çalışmada, öznel normların bir bilgi ve bilgisayar güvenliği koruyucu davranışı olan siber hijyen üzerindeki etkisi araştırılmak istenmiştir. Bu nedenle aşağıdaki hipotez önerilmiştir:

H6: Öznel normlar, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyecektir.

Alışkanlıklar, belirli hedeflere ulaşmak için gerekli olan öğrenilmiş eylemler dizisi olarak tanımlanmaktadır (Verplanken ve Orbell., 2003). Genellikle rutin olarak tetiklenen refleks veya otomatik davranışlardır (Alraja vd., 2023). Bilgi sistemleri bağlamında güvenlik alışkanlığı, insanların öğrenme nedeniyle bilgi güvenliği davranışlarını otomatik olarak gerçekleştirme eğiliminin derecesi olarak tanımlanmaktadır (Lamayem vd., 2007). Alışkanlıkların rolüne ilişkin önceki çalışmalarda, bilgi güvenliği teorik modeline alışkanlık dahil edildiğinde açıklanan varyansı arttığı bulunmuştur (Sommestad vd., 2019; Zhang vd., 2009). Ayrıca, alışkanlıklarla ilgili mevcut literatür, organizasyonel hiyerarşiye ve güvenlik politikalarına sahip büyük organizasyonlara odaklanmıştır. Örneğin Pahnla vd. (2007), alışkanlığın çalışanların bilgi güvenliği politikalarına uyma niyetini olumlu yönde etkilediğini bulmuşlardır. Benzer şekilde başka bir çalışmada alışkanlığın çalışanların tehdit ve başa çıkma değerlendirme sürecini önemli ölçüde etkilediğini ve güvenlik politikalarına uyma niyetini etkilediği bulunmuştur (Vance vd.,

2012). Moody vd. (2018) alışkanlığın, çalışanların bilgi güvenliği politikalarına uyma konusundaki davranışsal niyetini güçlü bir şekilde açıkladığını tespit etmiştir. Benzer şekilde Aigbefo vd. (2022) tarafından yapılan çalışmada, kobi çalışanlarının güvenlik davranışı niyetlerinde alışkanlıkların güçlü bir etkisi olduğu bulunmuştur ($\beta = 0.420$). Ancak Alraja vd. (2023) tarafından yapılan çalışmada alışkanlıkların çalışanların bilgi güvenliği politikalarına uyum niyeti üzerinde anlamlı bir etkisinin olmadığı bulunmuştur. Ayrıca söz konusu bu çalışmalardaki yazarlar çelişen bulgular nedeniyle alışkanlıkların etkilerine ilişkin daha fazla çalışma yapılmasını önermektedir.

Literatürdeki bulgular, alışkanlığın potansiyel olarak bireyin güvenlik davranışı niyetini etkileyebileceğini göstermektedir. Çalışanların işle ilgili olmayan kendi kişisel güvenliğini sağlamadaki alışkanlığı, işle ilgili bağlamlarda siber güvenlik ile ilgili davranışsal niyetlerini etkileyebilir. Bu doğrultuda çalışanların koruyucu güvenlik eylemlerini gerçekleştirme alışkanlığı ne kadar güçlüyse, koruyucu güvenlik eylemleri gerçekleştirme niyetinin de o kadar büyük olacaktır. Bu nedenle literatürdeki bulgulardan da hareketle aşağıdaki hipotez önerilmiştir:

H7: Alışkanlıklar, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyecektir.

Belirli bir davranışa yönelik tutum, bir kişinin söz konusu davranışa ilişkin olumlu veya olumsuz değerlendirme veya değerlendirmelerinin derecesini ifade eder (Bélanger vd., 2017). Bilgi güvenliği literatüründe güvenlik politikasına yönelik tutum, son kullanıcıların kurumsal bilgi sistemleri güvenlik politikaları hakkındaki olumlu veya olumsuz görüşü olarak tanımlanmaktadır (Guo vd., 2011). Tutum ve davranışsal niyet arasındaki ilişki bilgi sistemleri literatüründe geniş çapta test edilmiştir (Venkatesh vd., 2003).

Literatürdeki çalışmalar, bilgi sistemleri güvenlik politikalarına uymaya yönelik tutumların davranışsal niyetleri olumlu yönde etkilediğini göstermiştir (Bulgurcu vd., 2010; Pahnla vd., 2007; Myyry vd., 2009; Herath ve Rao, 2009a; Ifinedo 2018; D’Arcy ve Lowry 2019).

Bu çalışmada tutum, bir çalışanın güvenlik prosedürlerine yönelik olumlu veya olumsuz düşüncelerini ifade etmektedir. Bilgi sistemleri güvenlik politikalarına yönelik olumlu tutum, bilgi güvenliği ile ilgili davranışsal niyeti üzerinde artı etkiye sahiptir. Tersine, olumsuz tutumlar ise, davranışsal niyeti azaltacaktır. Dolayısıyla, kurumlarının bilgi

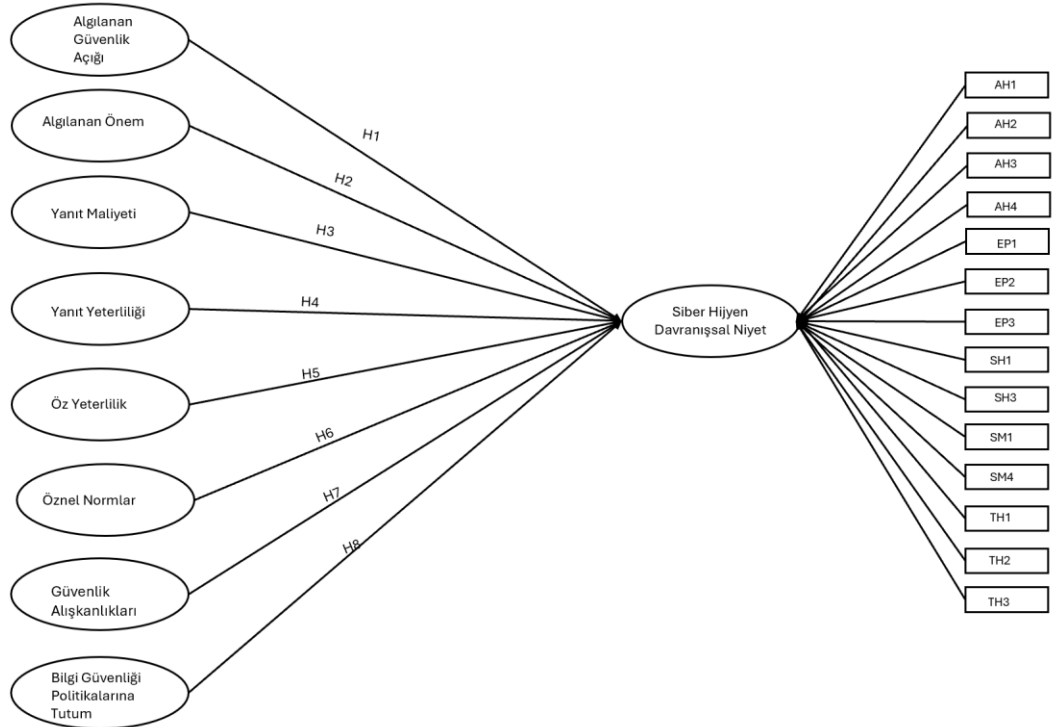
sistemleri güvenlik politikaları hakkında olumlu görüş ve değerlere sahip bireyler, bu tür kurallara ve yönergeler uyma konusunda olumlu eğilimlere sahip olacaklardır (Sasse vd., 2004; Ng vd., 2009; Herath ve Rao, 2009a; Bulgurcu vd., 2010). Öte yandan, olumlu tutumlara sahip olmayanlar politikalara hemen uyum sağlayamayacaktır (Pahnila vd., 2007; Myrty vd., 2009; Sheeran vd. 2016). Bu nedenle, BT çalışanlarının güvenlik politikalarına yönelik tutumunun, siber hijyen davranışsal niyeti etkileyeceği önerilmiştir. Böylece:

H8: Bilgi güvenliği politikalarına karşı tutum, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyecektir.

Araştırmanın hipotezleri, Şekil 17’de yer alan araştırma modelinin üzerinde gösterilmektedir.

Şekil 17

Araştırma Modeli



3.4. Anakütle ve Örneklem

Sosyal bilim araştırmalarında, araştırmacılar yapacakları araştırma sonuçları genelleyecekleri evrendeki birimlerin tamamına ulaşmaları her zaman mümkün olmayabilir. Zaman, maliyet, emek ve diğer nedenlerden dolayı araştırmacıların evrendeki tüm birimleri gözlemleyebilmesi olanaklı değildir. Bu nedenle araştırmacılar,

evreni temsil etme yeteneđi en iyi olan örneklemeler üzerinden çalışarak araştırmalarını yürütmektedirler (Gürbüz ve Şahin, 2018).

Çalışmanın ana kütesini, Türkiye’deki 18 yaş üzeri uzaktan veya hibrit şeklinde çalışanlardan oluşturmaktadır. Ancak bu tanımlama kapsamında yer alan çalışanların tamamına ulaşmanın zor olması ve çalışmanın kaynaklarının kısıtlı olması sebebiyle örneklem yapması uygun görülmüştür.

Araştırmanın verilerinin toplanması, tesadüfi olmayan örneklem tekniklerinden amaçlı örneklem tekniđi kullanılarak yapılmıştır. Amaçlı örneklem, araştırmacı kişisel gözlemlerinden hareketle araştırma problemine uygun olduğunu düşündüğü belirli özellikleri taşıyan katılımcıların seçildiđi örneklem yöntemidir. Araştırma amacına en uygun katılımcılar örneklem dahil edilmektedir (Gürbüz ve Şahin, 2018).

Çalışma evreninin daraltılması adına çalışmanın kaynakları ve imkanların dahilinde örneklem seçileceđi sektör sadece bilişim sektörü olarak belirlenmiştir. Bilişim sektörü uzaktan ve hibrit şeklinde çalışmaya diđer sektörlere kıyasla daha yatkın olması nedeniyle seçilmiştir. Ayrıca dijital okuryazarlık derecesinin daha yüksek olması, organizasyon içinde kritik görevlerde bulunması ve bilgi kaynaklarına erişim yetkilerinin sınırsız olması sebebiyle de seçilmiştir. Kritik görevlerde bulunan ve işletme bilgilerine tam erişimi olan çalışanların siber hijyeni diđer sektör çalışanlara kıyasla daha önemlidir. Çünkü bu çalışanlar BT varlıklarına ve değerli bilgilere en fazla erişime sahip olan çalışanlardır ve bu nedenle siber saldırganların hedefi olmaktadır (Greengard, 2016; Torton vd., 2018). Dolayısıyla siber hijyen seviyelerine dikkat edilmesi gereken en önemli sektördür.

Örneklem kapsamının belirlemesinden sonra araştırmacı, ne kadar büyüklükteki örneklem sayısına ihtiyacı olduğunu tespit etmelidir. Belirlenecek örneklem büyüklüğünün, araştırmacının zaman ve maliyet olanaklarına uygun olması gerekmektedir. Nicel araştırmalarda örneklem büyüklüğü konusunda dikkat edilecek bazı hususlar bulunmaktadır. Örneklem büyüklüğü verilerle yapılacak olan analiz türüne göre değişmektedir (Gürbüz ve Şahin, 2018). Faktör analizi yapılacak ise ölçekteki her bir madde sayısının yaklaşık 10 katı kadar bir örneklem ile çalışılması gerekmektedir (Büyüköztürk, 2005; Rubin ve Er, 2011). Fakat bu sayı üzerinde ortak bir fikir birliđi yoktur. Bazı araştırmacılar örneğin Guilford (1954) örneklem boyutunun 200 olmasının faktör analizi için yeterli olduğunu savunmaktadır. (Gorsuch, 1983) ve (Hatcher, 1994)

ise faktör analizinde örneklem boyutunun ölçekteki ifade sayısının 5 katı olarak belirlenmesinin yeterli olacağını savunmaktadır. Kline (2011) göre ise örneklem büyüklüğünün ölçekteki madde sayısının 10 katı olması ve bu sayının da 200'den az olmaması gerektiği savunmaktadır. Yapısal eşitlik modellemesi yapılacak olan araştırmalarda asgari örneklem sayısı 200 olarak kabul edilmektedir (Barrett, 2007; Hoelter, 1983; Kline, 2011). Sekaran ve Bougie (2016, s. 264) göre ise tahmini ana kütlenin 1 milyon ve üzeri olması durumunda örneklem büyüklüğü için 384 sayısı yeterli kabul edilmektedir. Özetle örneklem büyüklüğü genellikle minimum 200 ile 500 arasında değişmektedir.

Bu araştırmada, örneklem büyüklüğüne dair verilen tüm bilgilerden hareketle örneklem sayısının belirlenmesinde ölçekteki madde sayısı dikkate alınmıştır. Ölçüm aracında 50 maddelik ifade havuzu olduğundan $50 \times 10 = 500$ katılımcılıya ulaşılması hedeflenmiştir. Bu hedef doğrultusunda toplam 535 uzaktan veya hibrit şeklinde çalışan BT uzmanı araştırmaya katılmıştır.

3.5. Enstrümanın Geliştirilmesi ve Veri Toplama Yöntemi

Anketin yapısal uyumu, soruların netliği ve anlaşılabilirliği ile araştırma amacına uygunluk açısından anket formu alan uzmanlarıyla birlikte detaylı bir incelemeden geçirilmiştir. Anket yapısı açısından soruların sıralanması ve sayfa düzeni üzerinde değişiklikler yapılmıştır. Katılımcıyı sıkmamak ve anket düzenini bozmayacak şekilde düzeltmeler yapılmıştır. Ölçek ifadelerinde anlatımı zayıflatacak teknik ve okuyucunun anlamasını zorlaştıracak kelimelerden uzak durulmaya çalışılmıştır. Soruların anlaşılabilirliğini artırmak için mümkün olduğunca genellemelerden kaçınılarak, konuyu net bir şekilde anlatacak kelimelerin kullanılmasına özen gösterilmiştir. Alan uzmanları ile yapılan görüşmede ortaya çıkan, birbiriyle benzerliği fazla olan ve ayırım özelliği yetersiz olduğu düşünülen 3 madde ifade havuzundan çıkarılmıştır. Nihai ölçek 53 ifadeden 50 ifadeye düşmüştür.

İfade havuzunda kalan 50 ifade görünüm geçerliliği açısından değerlendirildiğinde ise; ifadelerin net anlaşılması ve akıcılığın sağlanması adına uzman görüşleri alındıktan sonra 21 ifadede bazı iyileştirmeler yapılmıştır.

Nihai olarak elde edilen 50 ifadelik havuza yaş, cinsiyet, eğitim durumu gibi demografik değişkenler eklenmesine karar verilmiştir. Literatüre bakıldığında koruma motivasyon

teorisi ölçeklerinde genellikle 5’li Likert ölçeği kullanıldığı incelenmiş olup bu anket içinde tamamen katılıyorum ve kesinlikle katılmıyorum likert ölçeği uygun görülmüştür.

Tablo 2

Modeldeki Faktörlerin Kaynakları

Faktör Adı	Kaynak
Güvenlik Alışkanlıkları	(Tsai vd., 2016; Venkatesh vd., 2012)
Bilgi Güvenliği Politikasına Tutum	(Ifinedo, 2012)
Algılanan Önem	(Ifinedo, 2012; L. Li vd., 2022; Thompson vd., 2017a)
Algılanan Güvenlik Açığı	(Ifinedo, 2012; L. Li vd., 2022; Thompson vd., 2017a)
Yanıt Maliyeti	(Ifinedo, 2012; L. Li vd., 2022; Thompson vd., 2017a)
Yanıt Yeterliliği	(Ifinedo, 2012; L. Li vd., 2022; Thompson vd., 2017a)
Öz Yeterlilik	(Ifinedo, 2012; L. Li vd., 2022; Thompson vd., 2017a)
Öznel Normlar	(Ifinedo, 2012)
Siber Hijyen Davranışsal Niyet	(Karayel vd., 2024; Vishwanath vd., 2020)

Pilot Çalışma

Birinci aşama sonucunda elde edilen 50 ifade enstrüman görünüm geçerliliği bakımından uzaktan veya hibrit çalışan 25 kişiye online olarak uygulanan anket ile test edilmiştir. Test aşamasından cevaplayıcılardan her bir ifadeyi açıklık, anlaşılabilirlik, konuya uygunluk, cevaplama için gerekli zaman açısından değerlendirmeleri talep edilmiştir.

Pilot çalışma sonucunda katılımcılardan elde edilen geri bildirimler neticesinde ifade havuzundan herhangi bir ifadenin çıkarılmasına gerek olmadığı anlaşılmıştır. Katılımcılar anket hakkında yapılan yorumlarda; ifadelerde anlaşılması zor teknik ifadelerin olmadığını ve 10 dakikalık bir zaman diliminin anketi doldurmada yeterli olduğunu belirtmişlerdir.

Veri Toplama Yöntemi

Araştırma modelinin test edilmesi için gerekli verilerin toplanması aşamasında veri toplama yöntemi olarak birincil veri toplama kaynaklarından olan anket yöntemi tercih edilmiştir. Uzaktan çalışanlarının bulunmasının ve birebir görüşmenin zor olacağı nedeniyle veriler **Linkedin** platformu üzerinden toplanmıştır. **Linkedin** platformu üzerinden Türkiye’de yaşayan, bilişim sektöründe uzaktan veya hibrit şeklinde çalışan 18 yaş ve üzeri bireylere çevrimiçi anket uygulanmıştır. Veri toplama işlemi 15.08.2023-15.11.2023 tarihleri arasında, gönüllü katılımcılardan gerçekleştirilmiştir. Veri toplama için Sakarya Üniversitesi Etik Komisyonundan gerekli etik kurul onayı alınmış olup ilgili karar Ek-2’de sunulmuştur.

3.6. Yapısal Eşitlik Modellemesi

Nedensel modelleme teknikleri yol analizi ve yapısal eşitlik modeli olmak üzere iki türe ayrılmaktadır (Mertler ve Vannatta, 2005) Yol analizi yalnızca gözlemlenen değişkenleri dikkate alır ve nedensel bir akış kurar. Yol analizi kullanılarak hem doğrudan hem de dolaylı etkiler tahmin edilebilir. Yapısal eşitlik modeli ise, faktör analizi ve yol analizinin kapsamlı bir istatistiksel metodolojide birleşimini temsil eder. Gözlemlenen ve gizil değişkenleri dikkate alır ve yol analizine göre birçok avantaja sahiptir (Kaplan, 2008). YEM, genellikle bir teoriyi veya modeli test etmek için kullanılan doğrulayıcı bir yöntemidir. Bu nedenle değişkenler arasındaki potansiyel ilişkilere yönelik teori veya hipotezlere ilişkin ön bilgi gereklidir (Tabachnick ve Fidell, 2007).

Yapısal Eşitlik Modellemesi CB-SEM ve PLS-SEM olmak üzere ikiye ayrılır. CB-SEM kovaryans temelli iken, PLS-SEM varyans temellidir. Amos ve Lisrell gibi paket programlar CB-SEM mantığında, Smart-PLS ise PLS-SEM mantığındaki paket programdır. CB-SEM daha popüler bir yöntem olmasına rağmen; PLS-SEM daha yeni ve sıklıkla kullanılan bir yöntemdir. Pazarlama, stratejik yönetim, yönetim bilişim sistemleri ve muhasebe gibi birçok sosyal bilim alanlarında alanda PLS-SEM kullanan araştırmaların sayısı artmaktadır (Hair vd., 2014).

Tablo 3*PLS-SEM vs CB-SEM Karşılaştırması*

Model Gereksinimi	PLS-SEM	CB-SEM
Etkileşim etkileri içerir	Kolay etkileşim etkileri için tercih edilebilir	Küçük modellerde yapılması zordur
Formatif değişken etkileri	Kolay	Zor
Çoklu grup moderatör değişkenler	Kullanılabilir fakat zor	Kullanılabilir
Alternatif modeller test etme	Kullanılabilir	Model uyum istatistikleri sağladığı için tercih edilebilir
Değişken sayısı (40 +)	Tercih edilebilir	Güvenilir olmayabilir
Normalliğin olmaması	Kullanılabilir	Kullanılmamalı; güvenilirmez
Varyansın homojen olmaması	Kullanılabilir	Kullanılmamalı; güvenilirmez bulgularla sonuçlanabilir
Küçük örneklem	Kullanılabilir	Kullanılmamalı; güvenilirmez bulgularla sonuçlanabilir

Kaynak:(Lowry ve Gaskin, 2014)

PLS örneklem büyüklüğü, homojenlik ve normal dağılım için daha az zorlayıcı koşullar vardır (Hair vd., 2014). PLS'nin, tahmin ve teori geliştirme söz konusu olduğunda, belirli bir istatistiksel düzeye ulaşmak için CB-SEM'in yalnızca yarısı kadar gözleme ihtiyaç duyduğunu öne sürülmektedir (Reinartz vd., 2009). CB-SEM kullanıldığında model uyumunun doğru bir şekilde değerlendirilmesi için Hoelter (1983) tarafından en az 200'lük bir örneklem büyüklüğü önerilmiştir. Öte yandan PLS, genellikle daha küçük örneklem boyutlarıyla ve normal dağılım varsayımının şüpheli olduğu durumlarda uygulanabilmektedir (Gefen, Straub ve Rigdon, 2011).

Smart-LS yazılımını yapısal eşitlik modelleme aracı olarak kullanmanın temel amacı, bağımlı değişkenler olarak bilinen endojen gizli yapıların açıklanan varyansını maksimuma çıkarmaktır. Smart-PLS, programı kısmı en küçük kareler yöntemini kullanır. Amos ve Lisrell gibi programlarla karşılaştırıldığında kullanımı oldukça kolay ve kullanıcı dostu programdır (Yıldız, 2021, s. 21–22).

Smart-PLS kullanmanın en önemli üç nedeni, normal olmayan veriler üzerindeki esneklik, küçük örneklem büyüklüğü ve formatif göstergelerin dahil edilmesidir (Hair vd, 2014). Smart-PLS'nin CB-SEM temelli yapısal eşitlik modellemesine göre avantajları, örneklem büyüklüğü konusunda daha az kısıtlamaya sahip olması, normal dağılımlı verilerin gerekli olmaması, çok sayıda formatif ve reflektif yapıları içeren karmaşık modeli analiz edebilmesidir. Ayrıca amaç endojenin açıklanan varyansını en üst düzeye çıkarmak olduğunda da PLS-SEM kullanılmaktadır (Urbach ve Ahlemann, 2010).

Sonuç olarak, bu çalışmada araştırma modeli formatif ve reflektif yapılar içermektedir. Ayrıca araştırmada küçük örneklem sayısı tercih edilmiştir. Tüm bu nedenler dikkate alındığında CB-SEM tabanlı yazılım yerine Smart-PLS'nin tercih edilmesinin daha doğru olacağı düşünülmektedir.

BÖLÜM 4. ANALİZ VE BULGULAR

Bu bölümde, analiz sonuçlarına ve bulguların değerlendirmelerine yer verilmiştir. Çalışma bağlamında uzaktan ve hibrit çalışanlar olmak üzere iki grup üzerinden saha çalışması yürütülmüştür. İlk olarak ankete katılan 535 cevaplayıcının cinsiyet, yaş, eğitim durumu ve gelir düzeylerine ilişkin olmak üzere tanımlayıcı bilgiler olarak nitelendirilen demografik bilgilere yer verilmiştir. Sonrasında açıklayıcı faktör analizi, farklılık analizleri, Smart-PLS analizleri ve son olarak da hipotez testlerine yer verilmiştir.

4.1. Demografik İstatistikler

Bu başlık altındaki analizler, önce genel bilgiler sonrasında uzaktan çalışan ve hibrit şeklinde çalışanlara yönelik olarak sunulmuştur. Uzaktan çalışan 262, hibrit şeklinde çalışan 273 ve toplamda 535 katılımcıdan oluşan bir veri seti üzerinden analizler gerçekleştirilmiştir. Çalışma kapsamında yer alan ve BT çalışanı olan katılımcıların demografik özellikler *Tablo 4'* te sunulmuştur.

Tablo 4

Tüm Katılımcıların Demografik Özellikleri

Demografik Özellikler	Frekans	%
<u>Yaş</u>		
18-24	109	20,4
25-34	333	62,2
35-44	67	12,5
45-54	13	2,4
55-64	13	2,4
Toplam	535	100,0
<u>Cinsiyet</u>		
Kadın	159	29,7
Erkek	376	70,3
Toplam	535	100,0
<u>Eğitim</u>		
Lise	29	5,4
MYO	23	4,3
Lisans	347	64,9
Yüksek Lisans	87	16,3
Doktora	49	9,2
Toplam	535	100,0

Tablolar Devamı

Gelir Düzeyi

15.000 TL ve altı	41	7,7
15.001-25.000 TL	129	24,1
25.001-35.000 TL	151	28,2
35.001-45.000 TL	82	15,3
45.001 TL ve üzeri	132	24,7
Toplam	535	100,0

Tablo 4'e göre katılımcıların demografik özellikleri incelendiğinde, büyük bir çoğunluğunun (%62,2) 25- 34 yaş arasında, %20,4 'ünün 18-24 yaş aralığında ve 12,5%'inin 35-44 yaş aralığında olduğu görülmektedir. Katılımcıların %70,3 erkek, %29,7 kadındır. Eğitim durumu açısından katılımcıların dağılımı incelendiğinde büyük bir çoğunluğunun (%64,9) lisans seviyesinde olduğu görülmektedir. Gelir düzeylerine bakıldığında, katılımcıların dağılımının hemen hemen birbirine yakın olduğu görülmektedir.

Tablo 5

Uzaktan Çalışan Katılımcıların Demografik Özellikleri

Demografik Özellikler	Frekans	%
<u>Yaş</u>		
18-24	70	26,7
25-34	161	61,5
35-44	29	11,1
45-54	1	0,4
55-64	1	0,4
Toplam	262	100,0
<u>Cinsiyet</u>		
Kadın	77	29,4
Erkek	185	70,6
Toplam	262	100,0
<u>Eğitim</u>		
Lise	16	6,1
MYO	11	4,2
Lisans	195	74,4
Yüksek Lisans	37	14,1
Doktora	3	1,1
Toplam	262	100,0

Gelir Düzeyi		
15.000 TL ve altı	24	9,2
15.001-25.000 TL	62	23,7
25.001-35.000 TL	67	25,6
35.001-45.000 TL	38	14,5
45.001 TL ve üzeri	71	27,1
Toplam	262	100,0

Tablo 5'e göre uzaktan çalışan katılımcıların demografik özellikleri incelendiğinde, büyük bir çoğunluğunun (%61,5) 25- 34 yaş arasında, %26,7 'sinin 18-24 yaş aralığında ve 11,1%'inin 35-44 yaş aralığında olduğu görülmektedir. Katılımcıların %70,6 erkek, %29,4 kadındır. Eğitim durumu açısından katılımcıların dağılımı incelendiğinde büyük bir çoğunluğunun (%74,4) lisans seviyesinde olduğu görülmektedir. Gelir düzeylerine bakıldığında, katılımcıların dağılımının hemen hemen birbirine yakın olduğu görülmektedir.

Tablo 6*Hibrit Şeklinde Çalışan Katılımcıların Demografik Özellikleri*

Demografik Özellikler	Frekans	%
<u>Yaş</u>		
18-24	39	14,3
25-34	172	63,0
35-44	38	13,9
45-54	12	4,4
55-64	12	4,4
Toplam	273	100,0
<u>Cinsiyet</u>		
Kadın	82	30,0
Erkek	191	70,0
Toplam	273	100,0
<u>Eğitim</u>		
Lise	13	4,8
MYO	12	4,4
Lisans	152	55,7
Yüksek Lisans	50	18,3
Doktora	46	16,8
Toplam	273	100,0

Gelir Düzeyi		
15.000 TL ve altı	17	6,2
15.001-25.000 TL	67	24,5
25.001-35.000 TL	84	30,8
35.001-45.000 TL	44	16,1
45.001 TL ve üzeri	61	22,3
Toplam	273	100,0

Tablo 6' ya göre hibrit şekilde çalışan katılımcıların demografik özellikleri incelendiğinde, büyük bir çoğunluğunun (%63,0) 25- 34 yaş arasında, %14,3 'ünün 18-24 yaş aralığında ve 13,9%'inin 35-44 yaş aralığında olduğu %8,8'inin 45-64 yaş aralığında olduğu görülmektedir. Katılımcıların %70 erkek, %30 kadındır. Eğitim durumu açısından katılımcıların dağılımı incelendiğinde büyük bir çoğunluğunun (%55,7) lisans seviyesinde olduğu görülmektedir. Gelir düzeylerine bakıldığında, katılımcıların %55,3'ünün 15.000 ile 35.000 arasında bir gelire sahip olduğu, %6,2'sinin 15.000 ve altı gelire, %16,1'inin 35.001- 45.000 arasında bir gelire ve %22,3'ünün 45.001 ve üzeri gelire sahip olduğu görülmektedir.

4.2. Güvenilirlik Analizi

Sosyal bilim araştırmalarında faktör analizi yapılmadan önce ölçek maddeleri arasında tutarlılık olup olmadığı belirlenmesi gerekmektedir. Diğer bir deyişle iç tutarlılık analizi (güvenilirlik analizi) yapılması önerilmektedir. İç tutarlılık analizi, ölçümlerin tutarlılığı görebilmek için yapılmaktadır. Bir ölçme aracındaki tüm maddelerin aynı amaca hizmet edip etmediğini belirlemek ve maddelerin bir bütün oluşturup oluşturmadığını görmek amacıyla uygulanmaktadır (Büyüköztürk, 2005; Gürbüz ve Şahin, 2018).

Bu çalışmada kapsamında ilk olarak ölçeğe iç tutarlılık testi yapılmış olup, Cronbach Alfa değeri 0.939 olarak bulunmuştur. Ayrıca madde toplam korelasyon değerleri de hesaplanmıştır. Literatürde Cronbach Alfa (α) değerlerinin kabulü için eşik değer olan 0,70'ten yüksek olması istenmektedir (Büyüköztürk, 2005; Gürbüz ve Şahin, 2018; J. F. Hair vd., 2014).

Tablo 7*Ölçek İfadelerinin İç Tutarlılık Analizi Sonuçları*

İfadeler	Madde- Toplam Korelasyonu	Madde Çıkarıldığı nda Cronbach Alfa
<u>Alışkanlıklar</u>		
Güvenlik önlemlerini uygulamak benim için bir alışkanlık haline gelmiştir.	0,696	0,936
Güvenlik önlemlerini uygulamak düşünmeden yaptığım bir eylemdir.	0,530	0,936
Güvenlik önlemlerini uygulamak rutinimin bir parçasıdır.	0,749	0,937
<u>Bilgi Güvenliği Politikasına Tutum</u>		
Çalıştığım kurumun bilgi güvenliği politikasını takip etmek iyi bir fikirdir.	0.554	0.936
Çalıştığım kurumun bilgi güvenliği politikasını takip etmek bir zorunluluktur.	0.516	0.937
Çalıştığım kurumun bilgi güvenliği politikasını takip etmek faydalıdır.	0.557	0.936
<u>Algılanan Önem</u>		
Çalıştığım kurumun bilgilerini korumanın önemli olduğuna inanıyorum.	0.482	0.938
Şüpheli bir e-posta ekini açmam sonucunda bilgisayarıma virüs bulaşması benim için ciddi bir sorundur.	0.413	0.938
Çalıştığım kuruma yönelik gerçekleştirilen bilgi güvenliği ile ilgili siber saldırıları zarar verici görüyorum.	0.340	0.938
Bilgisayarımdaki bilgilerime iznim olmadan birinin erişmesi benim için ciddi bir sorundur.	0.380	0.938
Bilgisayarıma siber saldırı düzenlemesinden kaynaklanan veri kaybı benim için ciddi bir sorundur.	0.402	0.938
<u>Algılanan Güvenlik Açığı</u>		
Güvenlik önlemlerine yeterince dikkat etmezsem çalıştığım kurumun bilgileri tehlikeye girebilir.	0.520	0.937
Çalıştığım kurumun bilgilerini koruma çabamın, bu bilgilere yasa dışı erişimi azaltacağını düşünüyorum.	0.530	0.937
Bilgi güvenliği politikasına uymazsam, çalıştığım kurumun güvenlik ihlallerine karşı savunmasız hale gelebileceğini düşünüyorum.	0.479	0.938
Bilgi güvenliği politikasına uymazsam, çalıştığım kurumun siber saldırıların hedefi haline gelebileceğini düşünüyorum.	0.482	0.938
<u>Yanıt Maliyeti</u>		
Güvenlik Önlemlerini uygulamak çok zamanımı alıyor.	0.323	0.939
Güvenlik önlemlerini uygulamak beni rahatsız ediyor.	0.433	0.938

Tablolar Devamı

Güvenlik önlemlerini uygulama ile elde edilen faydaların, güvenlik önlemlerinin maliyetini karşılamadığını düşünüyorum.	0.405	0.938
Güvenlik önlemleri uygulamak iş yükümü artırıyor.	0.350	0.939
<u>Yanıt Yeterliliği</u>		
Güvenlik önlemlerini etkinleştirmek siber saldırılarını önlemenin etkili bir yoludur.	0.425	0.938
Güvenlik önlemlerini uygulamak kötü niyetli kişilerin kişisel veya finansal bilgilerime erişmesini engelleyecektir.	0.424	0.938
Çalıştığım kurumun bilgilerini güvenlik ihlallerinden korumak için alınan mevcut önlemler yeterlidir.	0.346	0.938
Kötü niyetli kişilerin kurumun bilgi sistemine erişimini önlemek için kullanabileceğim güvenlik önlemleri yeterlidir.	0.372	0.938
<u>Öz Yeterlilik</u>		
Kendimi bilgi güvenliği ihlallerinden korumak için gerekli bilgi ve becerilere sahibim.	0.643	0.936
Kötü niyetli kişilerin bilgilerime erişimini engellemek için önleyici tedbirler alacak uzmanlığa sahibim.	0.654	0.936
Kötü niyetli kişilerin bilgisayarına erişimini engellemek için önleyici tedbirler alma becerisine sahibim.	0.657	0.936
Bilgi güvenliği ihlallerinden korunmanın kendi kontrolümde olduğuna inanıyorum.	0.445	0.938
Gerekli kılavuzlar olduğunda bilgisayarımda güvenlik önlemlerini aktif hale getirebilirim.	0.559	0.937
Bilgi güvenliği önlemlerini uygulamak benim için kolaydır.	0.666	0.936
<u>Özel Normlar</u>		
Yöneticim güvenlik önlemlerini takip etmem gerektiğini düşünüyör.	0.552	0.937
Meslektaşlarım güvenlik önlemlerini takip etmem gerektiğini düşünüyör.	0.539	0.937
Bilgi-işlem departmanı güvenlik önlemlerini takip etmem gerektiğini düşünüyör.	0.513	0.937
Astlarım güvenlik önlemlerini takip etmem gerektiğini düşünüyör.	0.531	0.937
<u>Siber Hijyen Davranışsal Niyet (CHBI)</u>		
Herhangi bir yeni USB bellek veya harici depolama cihazında virüs taraması yaparım.	0.433	0.938
Virüs koruma yazılımını güncel tutarım.	0.504	0.937
Web sitesinin şifreleme kullanıp kullanmadığını görmek için tarayıcıdaki kilit simgesini kontrol ederim.	0.545	0.937
Çevrimiçi finansal işlemler yaparken SSL sertifikasının kalitesini kontrol ederim.	0.556	0.938
Halka açık internet ağlarında bilgisayarına 6 kişilerin elektronik ortamdaki erişimini yönetirim.	0.454	0.938

<i>Tablolar Devamı</i>		
Sosyal medya arkadaşlarımın ve onların bilgi taleplerinin güvenilirliğini değerlendiririm.	0.436	0.938
Sosyal medya platformlarında gizlilik ayarlarımı yönetirim.	0.447	0.938
İnternet erişimi olan tüm cihazlarda varsayılan şifrelerimi değiştiririm.	0.531	0.937
Karmaşık kullanıcı adları ve şifreler oluştururum.	0.576	0.937
Tüm çevrimiçi üyelikler için yeni / benzersiz kullanıcı adı ve şifreler oluştururum.	0.499	0.937
Oturumlar için iki faktörlü veya çok faktörlü kimlik doğrulamayı etkinleştiririm.	0.557	0.937
Gelen e-postanın başlığını kontrol ederim.	0.417	0.938
E-posta gönderen kişinin, e-posta alan adını kontrol ederim(e-postalardaki @ işaretinden sonraki kısım).	0.439	0.938
E-postalardaki isteklerde dilbilgisi veya yazım hatası olup olmadığını kontrol ederim.	0.387	0.938

Tablo 7 incelediğinde, ölçekten her bir madde çıkarıldığında Cronbach Alfa değerindeki meydana gelen değişikliğin çok yüksek oranlarda olmadığı tespit edilmiştir. Bu nedenle herhangi bir maddenin silinmesini gerektirmemiştir. Maddeler arası korelasyon değerleri incelediğinde eşik değer olan 0.30'un üzerinde değerler olduğu görülmektedir. Sonuç olarak, ölçeklerin iç tutarlılık güvenilirliği olduğu ayrıca ölçülmek istenen özelliğin doğru şekilde ölçüldüğünü ortaya konulmuştur.

4.3. Açıklayıcı Faktör Analizi

Faktör analizi, birbiri ile ilişkili n tane değişkeni bir araya getirerek az sayıda ilişkisiz ve kavramsal olarak anlamlı yeni faktörler bulmayı amaçlayan bir analiz türüdür. Başka bir ifadeyle, aynı yapıyı veya özelliği ölçen değişkenleri bir arada toplayarak ölçülen konuyu daha az sayıda boyutlarla açıklamayı amaçlayan istatistiksel yöntemdir (Büyüköztürk, 2005). Faktör analizi, bir değişken grubunu azaltmak veya maddeleri biraz daha küçük, daha yönetilebilir sayıda boyut veya faktörlerle bölmek amacıyla yapılmaktadır. Bunu birbiriyle ilişkili öğeleri aynı grup altında toplayarak yapmaktadır.

Faktör analizi için minimum örneklem gereksinimi vardır. Tabachnick ve Fidell (2007) faktör analizi için 5:1 oranını önermiştir. Her bir madde/ifade için 5 gözlem(katılımcı) istenmektedir. Bu doğrultuda ifade havuzunda toplamda 47 madde vardır. Açıklayıcı faktör analizi için gereken minimum örneklem büyüklüğü bu çalışma için 235' dir (47x5). Söz konusu bu çalışmanın ise toplam örneklem büyüklüğü 535 olduğundan, örneklem faktör analizi yapmak için yeterli olduğu değerlendirilmiştir.

Faktör analizinde verilerin faktör analizi için uygun olup olmadığı Kaiser-Meyer-Olkin (KMO) katsayısı ve Barlett küresellik testi ile incelenmektedir. KMO değeri, gözlenen korelasyon katsayılarının büyüklüğü ile kısmi korelasyon katsayılarının büyüklüğünü birbiriyle karşılaştıran bir test olarak ifade edilmektedir. Barlett testi, faktör analizi uygulanacak olan değişkenler arasında ilişki olup olmadığını kısmi korelasyonlar üzerinden incelemektedir. Barlett testi sonucunda hesaplanan ki-kare değerinin anlamlı çıkması verilerin faktör analizi için uygun olduğunu gösterir (Büyüköztürk, 2005; Coşkun vd., 2015).

Tablo 8

Örneklem Büyüklüğü İçin KMO Katsayıları

KMO Katsayısı	Örneklem Büyüklüğü
0,50-0,60	Kötü
0,60-0,70	Zayıf
0,70-0,80	Orta
0,80-0,90	İyi
0,90-1,00	Mükemmel

Kaiser-Meyer-Olkin (KMO) test sonucunun 0,50'den büyük olması beklenmektedir. Eğer test sonucunun 0,50'den küçük olması değişkenlerin faktör analizi için uygun olmadığını göstermektedir (Kaiser ve Rice, 1974). KMO test sonucu, değer 0,50'den düşük olması halinde faktör analizinin gerçekleştirilmesine devam edilmesi uygun görülmemektedir. Genel kanı ise KMO değerinin 0,60 ve üzeri olması halinde örneklemin faktör analizi için uygun olduğunu göstermektedir. Bartlett's küresellik testi ise korelasyon matrisindeki ilişkilerin faktör analizinin yapılabilmesi için yeterli olup olmadığını test etmektedir. Bu test sonucunun 0,05'ten küçük yani anlamlı olması halinde değişkenlerin faktör analizine uygun olduğunu ve faktör analizi yapılabileceği anlamı gelmektedir (Gürbüz ve Şahin, 2018).

Tablo 9

KMO Test Sonuçları

KMO	Bartlett's
0,904	0,000

Bu iki testin sonuçları Tablo 9'da rapor edilmiştir. Tablodaki sonuçlara göre Bartlett testinin tüm değerlerinin anlamlı olduğunu (p -değeri $< 0,05$) ve KMO değeri 0,904 olduğu tespit edilmiştir. Bu araştırma kapsamında her bir değişken literatürde yer edinmiş

ölçeklere ait ifadelerle ölçülmüştür. Araştırma kullanılan ölçeklerin yapı geçerliliklerini test etmek için faktör çıkarma ve döndürme yöntemi olarak Temel Bileşenler Analizi ve Varimaks Döndürme yöntemi kullanılmıştır. Açıklayıcı faktör analizi yapıldıktan sonra elde edilen faktör yükleri, her bir ifadenin ilgili faktör ile olan ilişkisini açıklayan bir katsayı olarak nitelendirilmektedir.

Tablo 10 incelendiğinde, ilk olarak algılanan güvenlik açığı ölçeğine ait faktör yüklerinin 0,629 ile 0,776 arasında değerler aldığı sonucuna ulaşılmıştır. Algılanan önem ölçeğine ait faktör yüklerinin 0,438 ile 0,767 arasında değerler aldığı görülmüştür. Yanıt maliyeti ait ifadelerin faktör yüklerinin 0,477 ile 0,893 arasında değerler almıştır. Yanıt yeterliliği ölçeğinde ait faktör yükleri 0,540 ile 0,847 arasında değişmektedir. Öz-yeterlilik boyutuna ait ifadelerin faktör yüklerinin 0,434 ile 0,903 arasında değerle aldığı tespit edilmiştir. Öznel normlar boyutuna ait ifadelerin faktör yüklerinin 0,783 ile 0,857 arasında değişmektedir. Alışkanlıklar ölçeğine ait ifadelerin faktör yüklerinin 0,529 ile 0,778 arasında oluşu ve Bilgi güvenliği politikasına tutum ölçeğine ait ifadelerin ise 0,468 ve 0,43 arasında olduğu ortaya konulmuştur.

Tablo 10

Faktör Yükleri

Boyutlar	Faktör 1	Faktör 2	Faktör 3	Faktör 4	Faktör 5	Faktör 6	Faktör 7	Faktör 8
PV1	0,776							
PV2	0,721							
PV3	0,663							
PV4	0,629							
PS1		0,767						
PS2		0,745						
PS3		0,651						
PS4		0,570						
PS5		0,438						
RC1			0,893					
RC2			0,840					
RC3			0,575					
RC4			0,477					
RE1				0,847				

Tablolar Devamı

RE2	0,819
RE3	0,694
RE4	0,540
SE1	0,903
SE2	0,871
SE3	0,788
SE4	0,655
SE5	0,553
SE6	0,434
SN1	0,857
SN2	0,855
SN3	0,810
SN4	0,783
HBT1	0,778
HBT2	0,530
HBT3	0,529
ISP1	0,843
ISP2	0,830
ISP3	0,468

Literatürdeki çalışmalar incelendiğinde Chou ve Chou (2016) ve Crossler ve Bélanger (2014) tarafından yapılan araştırmalarda güvenlik davranışını değişkeninin yordayıcı değişkenleri olarak algılanan duyarlılık, algılanan önem, öz yeterlilik, yanıt yeterliliği ve yanıt maliyeti olmak üzere toplamda beş temel faktör altında incelemiştir.

Geil vd. (2018) tarafından yapılan bir araştırmada siber güvenlik davranışı algılanan duyarlılık, algılanan önem, algılanan faydalar, öz yeterlilik ve eylem ipuçları olmak üzere beş faktörle ortaya koymuştur. Sulaiman vd.(2022) tarafından yapılan araştırmada siber güvenli davranışı algılanan duyarlılık, algılanan önem, algılanan engeller, güvenlik yanıt yeterliliği ve yanıt öz yeterliliği ile ölçmüştür.

BT çalışanları üzerine yapılan bir araştırmada, bilgi güvenliği koruma davranışları örgütsel bağlılık, iş tatmini, tehdit duyarlılığı, tehdit önemi, öz yeterlilik, yanıt maliyeti, tutum, algılanan davranış kontrol, öznel normlar olmak üzere dokuz faktör altında incelenmiştir (Ma, 2022). Yoon vd. (2012) tarafından yapılan bir araştırmada siber

güvenlik davranışsal niyeti algılanan duyarlılık, algılanan önem, öz yeterlilik, yanıt yeterliliği, yanıt maliyeti, öznel normal ve güvenlik alışkanlıkları ile ölçülmüştür.

Birleşik Krallık'ta çalışanlar üzerinde yapılan bir araştırmada siber güvenlik davranışı dokuz faktör altında incelenmiştir. Bu faktörler: algılanan maliyetler, sorumluluk, algılanan etkililik, algılanan önem, öz yeterlilik, bilgi güvenliği politikaları farkındalığı, önceki deneyim, bilgi güvenliğine duyulan ilgidir (Hanus vd., 2018). Yapılan bir araştırmada siber güvenlik davranışı algılanan duyarlılık, algılanan önem, öz yeterlilik, yanıt yeterliliği, yanıt maliyeti ve ödül olmak üzere altı değişken üzerinden incelemiştir (Crossler vd., 2019). Öğrenciler üzerinden yapılan bir araştırmada siber güvenlik davranışsal niyeti algılanan önem, algılanan duyarlılık, öz yeterlilik, yanıt yeterliliği, yanıt maliyeti, tehdit bilgisi, karşı önlem bilgisi ve algı faktörleriyle birlikte incelenmiştir (Khan vd., 2023).

Bu çalışmada elde edilen faktör sayısının literatürdeki bazı çalışmalarla paralellik göstermekte iken bazı çalışmalar ile farklılık göstermektedir. Genel olarak bu çalışma kapsamında kullanılan faktörlerin literatürle uyumlu bir şekilde bir araya geldiği görülmüştür.

4.4. Modele Ait Analizler

Araştırma modelinin analizinden önce araştırmada yer alan yapıların geçerlilik ve güvenilirlik çalışmaları gerçekleştirilmiştir. Geçerlilik ve güvenilirlik çalışmaları kapsamında iç tutarlılık güvenilirliği, birleşme geçerliliği ve ayrışma geçerliliği reflektif yapılar için değerlendirilmiştir. İç tutarlılık güvenilirliği için Cronbach Alfa ve Composite Reliability (CR) katsayıları incelenmiştir. Birleşme geçerliliğinin tespitinde faktör yükleri ile açıklanan ortalama varyans (AVE) değerleri incelenmiştir. Reflektif yapının aksine, formatif yapıların değerlendirmesi için katı kurallar yoktur. Ancak Hair vd. (2016), formatif yapıların yakınsak geçerliliği için kanonik korelasyon analizi yapılmasını önerirken, bazı popüler IS araştırmacıları, birbirleriyle ilişkilendirilmeleri gerekmediğinden yakınsak(convergent) ve ayırt edici(discriminant) geçerliliği yapmaya gerek olmadığını önermektedir (Lowry ve Gaskin, 2014; MacKenzie vd., 2011). Ek olarak, formatif göstergeler birbirleriyle pozitif, negatif korelasyonlu veya korelasyonsuz olabileceğinden Cronbach alfa, AVE gibi iç tutarlılık incelemeleri gerekli değildir (Bollen ve Lennox, 1991). Bunun yerine, formatif yapıların dış geçerliliği iki farklı yolla test edilmelidir (Diamantopoulos ve Winklhofer, 2001; Jarvis vd., 2003): doğrusallık

istatistikleri (collinearity statistics - outer VIF) ve faktör dış ağırlıklarına (outer weight) bakılması yeterli görülmektedir.

Sosyal bilim araştırmalarında eş doğrusallık probleminin olmaması adına VIF değerlerinin 5'in altında olması önerilmektedir (Hair vd., 2011). Outer Model VIF katsayıları formatif yapının geçerliliği için incelenmiştir. *Tablo 11'deki* VIF değerleri incelendiğinde indikatörlerin değerlerinin eşik değer olan 5'ten küçük olduğu görülmektedir. Buna göre formatif maddeler arasında doğrusallık problemi bulunmamaktadır.

Tablo 11

Formatif Maddelerin Dış VIF Değerleri

Maddeler	Dış VIF
AH1	1,772
AH2	2,462
AH3	2,021
AH4	1,754
EP1	1,816
EP2	1,756
EP3	1,447
SH1	1,498
SH3	1,466
SM1	1,476
SM4	1,553
TH1	1,841
TH2	1,867
TH3	1,533

Not: AH (Kullanıcı Bilgileri ve Şifre Hijyeni), EP (E-posta Hijyeni), SH (Saklama Alanı ve Cihaz Hijyeni), SM (Sosyal Medya Hijyeni), TH (Veri Aktarım Hijyeni)

Doğrusallığa bakıldıktan sonra formatif yapının geçerliliği için ikinci olarak kontrol edilen değerler ise t-istatistikleri, dış ağırlıklar ve dış yüklerdir. Hair vd. (2016), anlamlı olmayan dış ağırlık değerlerinin dış yüklerinin de kontrol edilmesini önermektedir. Dış yükler 0,5'ten yüksekse madde önemli kabul edilir. Dış yükün 0,5'ten düşük olması maddenin tamamen önemsiz olduğu anlamına gelmemektedir. Cenfetelli ve Bassellier (2009) formatif indikatörlerin teorik gerekçelerde haklı olunduğu sürece modelde tutulması gerektiği savunmaktadır. Bu nedenle, yazarlar formatif bir göstergeyi silme

konusunda dikkatli davranılması gerektiğini tavsiye etmektedir. Bunun sebebi silinmesine karar verilen maddenin ölçülmek istenilen özelliğin doğasını değiştirebilir nitelikte olmasıdır.

Tablo 12

Reflektif Değişkenlerin Inner- VIF Değerleri

Değişken Adı	VIF
Alışkanlıklar	2,262
Bilgi Güvenliği	1,696
Politikasına Tutum	
Algılanan Önem	1,514
Algılanan Güvenlik Açığı	1,745
Yanıt Maliyeti	1,219
Yanıt Yeterliliği	1,424
Öz Yeterlilik	2,097
Öznel Normlar	1,557

Tablo 12 reflektif yapının inner VIF değerlerini sunmaktadır. Reflektif yapının değişkenler arasındaki Inner-VIF değerleri incelendiğinde, en yüksek VIF değeri 2,097'dir. Tablodaki değerlerin eşik değer olan 5'in altında olmaması nedeniyle değişkenler arasında doğrusallık problemi olmadığı anlaşılmıştır.

Tablo 13

Formatif Yapının Dış Yükleri Ve Ağırlıkları

Maddeler	Dış Yükler	Dış Ağırlıklar	p
AH1	0,656	0,135	0,000
AH2	0,715	0,145	0,000
AH3	0,627	0,084	0,000
AH4	0,700	0,145	0,000
EP1	0,520	0,092	0,000
EP2	0,533	0,013	0,000
EP3	0,510	0,143	0,000
SH1	0,525	0,002	0,000
SH3	0,664	0,257	0,000

Tablolar Devamı

SM1	0,572	0,219	0,000
SM4	0,536	-0,002	0,000
TH1	0,670	0,077	0,000
TH2	0,703	0,214	0,000
TH3	0,561	0,050	0,000

Siber hijyen ölçeğinde faktör yüklerinin 0,50'den düşük çıkan 3 madde (SH2, SM2, SM3) ölçekten silinmiştir. *Tablo 13* formatif yapının her bir maddesinin dış ağırlıklarını ve yüklerini özetlemektedir. Burada AH (Kullanıcı Bilgileri ve Şifre Hijyeni), EP (E-posta Hijyeni), SH (Saklama Alanı ve Cihaz Hijyeni), SM (Sosyal Medya Hijyeni), TH (Veri Aktarım Hijyeni) 14 maddenin faktör yükleri 0,5' ten yüksek olduğu görülmektedir. Ayrıca faktör yüklerinin p değerlerinin eşik değer olan 0,05'ten küçük çıktığı yani p değeri istatistiksel olarak anlamlı çıktığı ortaya koyulmuştur.

Reflektif yapının geçerlilik ve güvenilirliği için Cronbach Alfa ve Composite Reliability (CR) ve AVE katsayıları incelenmiştir. Hair vd. (2014) göre faktör yükleri, Cronbach Alfa ve Composite Reliability değerlerinin 0,70 'ten büyük veya eşit olması gerekmektedir. Eğer faktör yükleri 0,40 ile 0,70 arasında ise ilgili faktörün bulunduğu yapının CR ve AVE değerlerinin kontrol edilmesi gerekmektedir. AVE değerinin ise 0,50'den büyük veya eşit olması beklenmektedir. Aşağıda yer alan tabloda araştırmada yer alan yapıların iç tutarlılık güvenilirliği ve birleşme geçerliliği ile ilgili sonuçlar yer almaktadır.

Tablo 14

Ölçüm Modeli Sonuçları

Değişken	İfade	Faktör Yükü	Cronbach's alpha	Composite reliability	AVE
Alışkanlıklar	HBT1	0,944	0,878	0,917	0,803
	HBT2	0,817			
	HBT3	0,921			
Bilgi Güvenliği Politikasına Tutum	ISP1	0,926	0,865	0,870	0,791
	ISP2	0,808			
	ISP3	0,928			
Algılanan Önem	PS1	0,740	0,825	0,834	0,586
	PS2	0,800			

Tablolar Devamı

	PS3	0,726			
	PS4	0,757			
	PS5	0,800			
Algılanan Güvenlik Açığı	PV1	0,845	0,859	0,863	0,702
	PV2	0,822			
	PV3	0,854			
	PV4	0,827			
Yanıt Maliyeti	RC1	0,702	0,783	0,828	0,584
	RC2	0,848			
	RC3	0,738			
	RC4	0,754			
Yanıt Yeterliliği	RE1	0,754	0,768	0,771	0,587
	RE2	0,788			
	RE3	0,753			
	RE4	0,769			
Öz Yeterlilik	SE1	0,866	0,892	0,907	0,658
	SE2	0,903			
	SE3	0,893			
	SE4	0,661			
	SE5	0,672			
	SE6	0,833			
Öznel Normlar	SN1	0,931	0,935	0,941	0,836
	SN2	0,930			
	SN3	0,887			
	SN4	0,908			
Siber Hijyen Davranışsal Niyet (CHBI)	AH1	0,656	0,871	0,890	0,523
	AH2	0,715			
	AH3	0,627			
	AH4	0,700			
	EP1	0,520			
	EP2	0,533			
	EP3	0,510			
	SH1	0,525			
	SH3	0,664			
	SM1	0,572			
	SM4	0,536			
	TH1	0,670			
	TH2	0,703			

Tablodaki değerler incelendiğinde reflektif yapıların faktör yüklerinin 0,661 ile 0,944 arasında gerçekleştiği görülmektedir. Hair vd. (2014)'e göre faktör yüklerinin ≥ 0.70 olmalıdır. Yazarlar, faktör yükleri 0,40 ile 0,70 arasında olan ifadelerin AVE ve ya CR değerlerinin eşik değerin altında olması durumunda modelden çıkarılmasını önermektedir. Hesaplanan AVE ve CR değerlerinin eşik değerlerin üzerinde olması sebebiyle faktör yükü 0.70'in altında olan reflektif yapıdaki ifadeler ölçüm modelinden çıkarılmamıştır. Formatif yapıdaki CHBI faktörünün ifadeleri faktör yüklerinin formatif yapılar için eşik değer olan 0.50'nin üstünde olduğu görülmektedir.

İç tutarlılık güvenirliği için Cronbach Alpha ve CR değerlerine bakılmıştır. Reflektif yapıların Cronbach Alpha katsayılarının 0,768 ile 0,935 arasında; CR katsayılarının da 0,786 ile 0,935 arasında gerçekleşmiş olması nedeniyle iç tutarlılık güvenirliğinin sağlandığı söylenebilir. Birleşme geçerliliği için reflektif yapıların faktör yükleri ile AVE değerlerine bakılmıştır. Reflektif yapıların faktör yüklerinin 0,661 ile 0,944 arasında; AVE katsayılarının da 0,586 ile 0,836 arasında gerçekleşmiş olması nedeniyle birleşme geçerliliğinin sağlandığı söylenebilir.

Ayrışma geçerliliği, bir yapının ampirik standartlara göre diğer yapılardan gerçekten ne ölçüde farklı olduğunu ifade eder (Hair vd. 2014). Ayrışma geçerliliği tespitinde, Fornell ve Larcker (1981) tarafından önerilen ölçüt ile Henseler vd. (2015) tarafından önerilen HTMT katsayıları kullanılmıştır. Ayrıca Chin (1998) tarafından önerilen çapraz yükler tablosu kullanılmıştır. Fornell ve Larcker (1981) ölçütüne göre, araştırmada yer alan yapıların açıklanan ortalama varyans (AVE) değerlerinin karekökü araştırmada yer alan yapılar arasındaki korelasyon katsayılarından yüksek olmalıdır. *Tablo 15'* te Fornell ve Larcker (1981) ölçütüne göre yapılan analiz sonuçlarına yer verilmektedir. Tablodaki değerler incelendiğinde, her bir yapının AVE karekök değerinin, diğer yapılarla olan korelasyon katsayılarından daha yüksek olduğu görülmektedir.

Tablo 15

Ayrışma Geçerliliği Sonuçları (Fornell Larcker Kriteri)

	HBT	ISP	PS	PV	RC	RE	SE	SN
Alışkanlıklar (HBT)	0,896*							
Bilgi Güvenliği Politikasına Tutum (ISP)	0,494	0,889*						

Tablolar Devamı

Algılanan Önem (PS)	0,314	0,357	0,765*					
Algılanan Güvenlik Açığı (PV)	0,371	0,479	0,547	0,838*				
Yanıt Maliyeti (RC)	-0,372	-0,273	-0,186	-0,207	0,764*			
Yanıt Yeterliliği (RE)	0,392	0,370	0,352	0,367	-0,298	0,766*		
Öz Yeterlilik (SE)	0,678	0,391	0,304	0,401	-0,361	0,459	0,811*	
Öznel Normlar (SN)	0,477	0,509	0,356	0,413	-0,203	0,311	0,351	0,914

Not:*AVE karekök değeri

Henseler vd. (2015) tarafından önerilen HTMT katsayıları, araştırmada yer alan tüm değişkenlere ait ifadelerin korelasyonlarının ortalamasının aynı değişkene ait ifadelerin korelasyonlarının geometrik oranlarını ifade etmektedir. Yazarlar, ölçmeye çalışılan yapıların teorik olarak birbirlerine yakın olmaları durumunda HTMT katsayılarının 0.90'ın; birbirlerinden teorik olarak uzak yapılarda ise 0.85'in altında çıkması gerektiğini belirtmişlerdir. *Tablo 16*'daki HTMT katsayıları incelendiğinde katsayıların eşik değerin altında olduğu görülmektedir.

Tablo 16

Ayrışma Geçerliliği Sonuçları (HTMT Kriteri)

	HBT	ISP	PS	PV	RC	RE	SE	SN
Alişkanlıklar (HBT)								
Bilgi Güvenliği Politikasına Tutum (ISP)	0,555							
Algılanan Önem (PS)	0,360	0,414						
Algılanan Güvenlik Açığı (PV)	0,408	0,554	0,635					
Yanıt Maliyeti (RC)	0,415	0,278	0,189	0,196				
Yanıt Yeterliliği (RE)	0,473	0,452	0,424	0,435	0,359			
Öz Yeterlilik (SE)	0,757	0,450	0,351	0,454	0,396	0,560		
Öznel Normlar (SN)	0,512	0,567	0,401	0,460	0,200	0,364	0,383	

Üçüncü ve son yaklaşım ise Chin'in (1998) öğelerin yüklenmesini çapraz kontrol eden çapraz yükleme kriterleridir. Bu yaklaşıma göre gizil bir değişken diğer yapıların öğelerinden ziyade kendi göstergeleri ile açıklanmalıdır.

Tablo 17*Çapraz Yükler Kriterinin Sonuçları*

	HBT	ISP	PS	PV	RC	RE	SE	SN
HBT1	0,944	0,460	0,291	0,342	-0,366	0,349	0,633	0,430
HBT2	0,817	0,326	0,244	0,217	-0,287	0,316	0,528	0,313
HBT3	0,921	0,511	0,302	0,403	-0,340	0,383	0,648	0,507
ISP1	0,431	0,926	0,321	0,428	-0,274	0,339	0,337	0,434
ISP2	0,446	0,808	0,307	0,432	-0,190	0,284	0,344	0,476
ISP3	0,442	0,928	0,325	0,417	-0,259	0,362	0,362	0,449
PS1	0,280	0,335	0,740	0,519	-0,260	0,298	0,248	0,299
PS2	0,236	0,279	0,800	0,426	-0,126	0,236	0,240	0,269
PS3	0,186	0,230	0,726	0,392	-0,117	0,261	0,169	0,226
PS4	0,268	0,236	0,757	0,332	-0,093	0,290	0,261	0,243
PS5	0,214	0,258	0,800	0,380	-0,072	0,255	0,232	0,306
PV1	0,337	0,409	0,458	0,845	-0,186	0,246	0,335	0,368
PV2	0,342	0,419	0,460	0,822	-0,200	0,372	0,395	0,305
PV3	0,257	0,386	0,479	0,855	-0,155	0,287	0,301	0,347
PV4	0,295	0,385	0,437	0,829	-0,148	0,328	0,304	0,365
RC1	-0,212	-0,091	-0,015	0,001	0,709	-0,176	-0,194	-0,056
RC2	-0,342	-0,284	-0,189	-0,230	0,849	-0,208	-0,317	-0,190
RC3	-0,297	-0,256	-0,220	-0,228	0,738	-0,305	-0,305	-0,232
RC4	-0,228	-0,084	-0,023	-0,030	0,754	-0,197	-0,232	-0,044
RE1	0,308	0,323	0,351	0,380	-0,272	0,754	0,332	0,272
RE2	0,281	0,276	0,345	0,358	-0,255	0,788	0,350	0,253
RE3	0,289	0,292	0,185	0,171	-0,175	0,753	0,332	0,205
RE4	0,323	0,241	0,163	0,177	-0,195	0,769	0,394	0,210
SE1	0,572	0,305	0,206	0,325	-0,317	0,409	0,866	0,263
SE2	0,623	0,300	0,224	0,335	-0,267	0,385	0,903	0,309
SE3	0,614	0,321	0,250	0,364	-0,293	0,361	0,893	0,312
SE4	0,435	0,264	0,165	0,251	-0,144	0,369	0,661	0,206
SE5	0,432	0,372	0,320	0,315	-0,296	0,338	0,672	0,284
SE6	0,588	0,345	0,308	0,346	-0,400	0,384	0,833	0,321
SN1	0,459	0,489	0,319	0,386	-0,167	0,266	0,354	0,931
SN2	0,442	0,474	0,324	0,401	-0,171	0,269	0,302	0,930

Tablolar Devamı

SN3	0,426	0,452	0,355	0,356	-0,194	0,307	0,307	0,887
SN4	0,415	0,443	0,312	0,366	-0,215	0,299	0,321	0,908

Ayrışma geçerliliği değerlendirme yöntemlerinden biri de, Çapraz Yükleme Kriteri olarak bilinen göstergelerin çapraz yüklemelerinin incelenmesidir. Bir gizil değişken kendi göstergelerinin varyansını diğer gizil değişkenlerin varyansından daha iyi açıklamalıdır. Böylelikle çoklu doğrusal bağlantı sorunu en aza indirilir (Chin, 1998). Bu aynı zamanda, bir göstergenin yüklerinin, kendisine atanmış yapıdan ziyade başka bir yapıya göre daha yüksek olmaması gerektiği anlamına da gelmektedir. Tabloda görüldüğü gibi tüm göstergeler en yüksek yükü gösterdikleri yapıda yer almaktadır. *Tablo 17* incelendiğinde her faktörün ilgili maddesi kendi satır ve sütununda yer alan diğer maddeler yüksek değere sahiptir. Yukarıda belirtilen üç tablodan hareketle ayrışma geçerliliği sağlanmıştır.

4.5. Araştırma Modeli ve Hipotez Testleri

Araştırmanın hipotezlerini test etmek amacıyla test edilen siber hijyen yapısının yol analizi sonuçları *Şekil 18*'de gösterilmiştir. Yol katsayısı yapılar arasındaki varsayılan ilişkileri temsil eder. Değerler -1 ile +1 arasında değişmektedir. $|1|$ 'e yakın bir değer güçlü bir ilişkiyi, sıfıra yakın bir değer ise anlamlı olmayan bir ilişkiyi belirtir. Değer aynı zamanda ilişkinin yönünü de (pozitif veya negatif) gösterir. Ancak bir katsayının anlamlı olup olmadığının belirlenmesi p değerine bağlıdır.

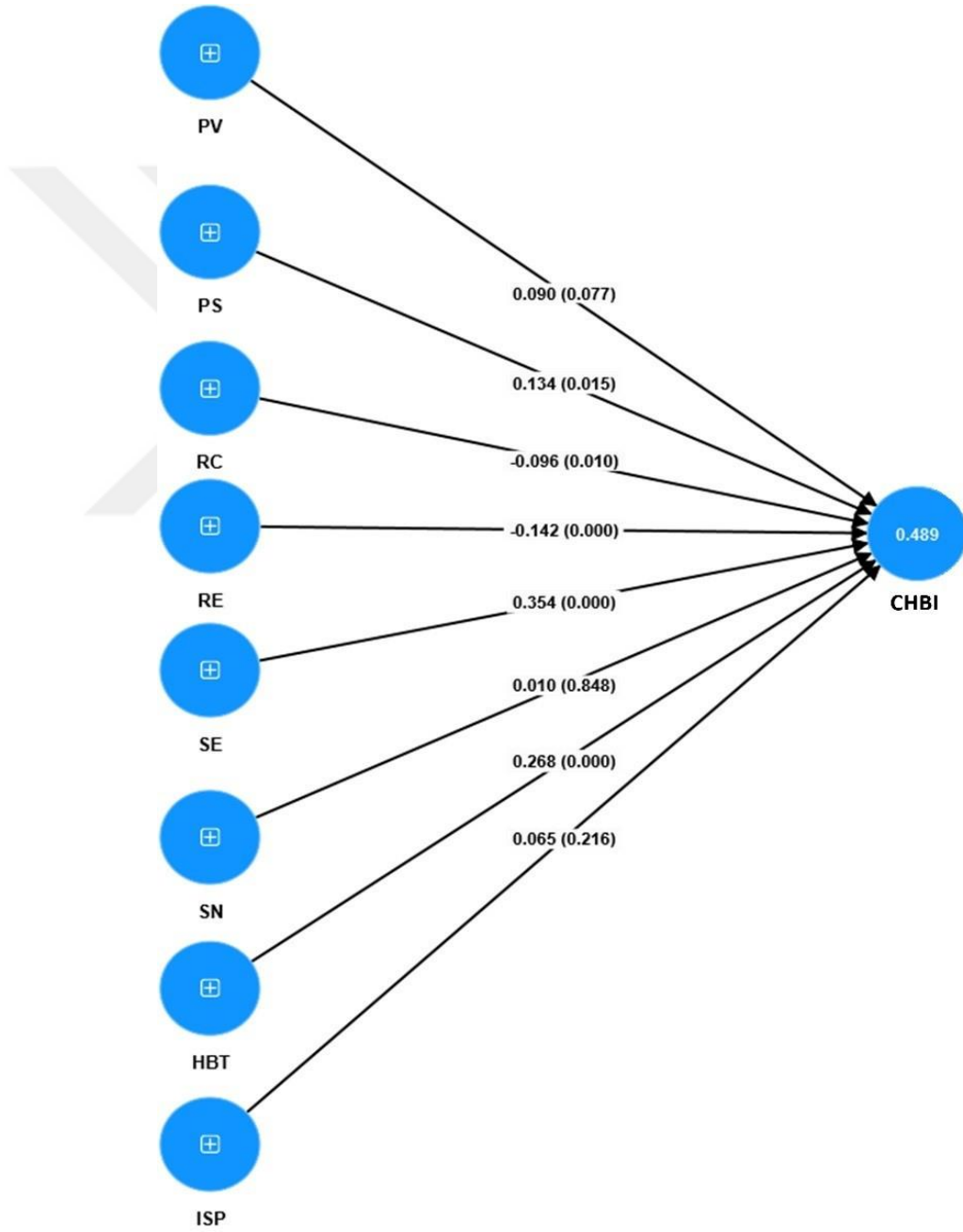
Yapısal bir model, gizil değişkenler arasında yapısal ilişkileri belirtmektedir (Hair vd., 2014). Bu doğrultuda *şekli 18*' de, araştırma kapsamında belirlenen ve incelenen yollar gösterilmiştir. Araştırma modelinde yer alan tek yönlü okların her biri araştırma hipotezlerini veya araştırma modelinde yer alan değişkenler arasındaki ilişkileri göstermektedir. Bu kapsamda incelenen yapısal ilişkilerdeki β değerlerinden siber hijyene en büyük etkiyi, öz yeterlilik (0,354) yaratmaktadır. Bu etkiyi ikinci olarak güvenlik alışkanlıkları (0,268) takip etmektedir. Algılanan önem, yanıt maliyeti, yanıt yeterliliği de siber hijyeni anlamlı bir şekilde yordamaktadır. Fakat önerilen model kapsamında algılanan güvenlik açığının, öznel normlar ve bilgi güvenliği politikasına karşı tutumun siber hijyen üzerindeki etkilerine ilişkin anlamlı bulgular elde edilememiştir. Dolayısıyla çalışanların siber hijyen davranışlarını algılanan güvenlik

açığının, öznel normların ve bilgi güvenliği politikasına tutumun etkilemediği tespit edilmiştir.

Elde edilen bulguların daha detaylı gösterimi (standardize β , t Değeri) *Tablo 20*'de sunulmuştur.

Şekil 18

Araştırma Modeli Smart-PLS Çıktısı



Yapısal modeli değerlendirmek için en yaygın kullanılan ölçü, R^2 katsayısıdır. R^2 , bağımsız değişkenler tarafından açıklanan bağımlı yapının varyansını gösterir ve

araştırma modelinin açıklayıcı gücünü ölçer (Shmueli ve Koppius, 2011). R^2 'nin değeri 0 ile 1 arasında değişir ve 1'e yakın olması güçlü bir tahmin gücüne işaret eder. Kabul edilebilir R^2 için genel bir kural yoktur. Farklı yazarlar *Tablo 18*'de gösterildiği gibi R^2 değerinin farklı değerlendirilmesini önermişlerdir.

Tablo 18

R^2 Değerlendirmesi

Chin (1998)	Cohen (1988)	Hair vd. (2011)	R^2 Değerlendirmesi
0,19	0,02	0,25	Zayıf
0,33	0,13	0,50	Orta
0,67	0,26	0,75	Güçlü

Tablo 19, araştırma modelinde gösterilen bağımsız değişkenlere ilişkin R-kare değerini göstermektedir. Modeldeki sekiz bağımsız değişken (algılanan önem, algılanan güvenlik açığı, yanıt maliyeti, yanıt yeterliliği, öz yeterlilik, alışkanlıklar, öznel normlar, bilgi güvenliği politikasına tutum) siber hijyen davranışsal niyetinin %48'ini açıklamaktadır.

Tablo 19

Model R^2 Değeri

	R^2	Düzeltilmiş R^2
CHBI	0,480	0,204

Test edilen hipotezlerin kabul ve ret durumları *Tablo 20*'de sunulmuştur. Ayrıca *Tablo 29*, PLS analizinden oluşturulan yol katsayılarını, t-istatistiğini ve p anlamlılık durumunu göstermektedir. BT çalışanlarına ait bulgular bir bütün olarak değerlendirildiğinde Hipotez 1, Hipotez 6 ve Hipotez 8 desteklenmemiştir.

Tablo 20

Yol Analizi Sonuçları

Hipotez	Standardize β	t Değeri	P	Sonuç
H1 Algılanan Güvenlik Açığı-> CHBI	0,090	1,770	0,077	Ret
H2 Algılanan Önem-> CHBI	0,134	2,425	0,015	Kabul
H3 Yanıt Maliyeti-> CHBI	-0,096	2,583	0,010	Kabul
H4 Yanıt Yeterliliği-> CHBI	-0,142	3,610	0,000	Kabul
H5 Öz Yeterlilik-> CHBI	0,354	6,685	0,000	Kabul
H6 Öznel Normlar-> CHBI	0,010	0,192	0,848	Ret
H7 Alışkanlıklar-> CHBI	0,268	4,834	0,000	Kabul

H8	Bilgi Güvenliği Politikasına	0,065	1,239	0,216	Ret
	Tutum-> CHBI				

Araştırma kapsamında önerilen hipotezler elde edilen bulgularla birlikte değerlendirilmiştir. H1 hipotezi ile *algılanan güvenlik açığının, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği* ifade edilmiştir. Bu hipotezin, 0,077 anlamlılık düzeyi, 1,770 t değeri ve 0,090 β katsayısı ile anlamlı olmadığı ortaya koyulmuştur. Bu nedenle H1 hipotezi reddedilmiştir. Siber hijyen üzerinde algılanan güvenlik açığının bir etkisi bulunmamaktadır.

H2 hipotezi ile *algılanan önemin, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği* ifade edilmiştir. Bu hipotezin, 0,077 anlamlılık düzeyi, 1,770 t değeri ve 0,090 β katsayısı ile anlamlı olduğu ortaya koyulmuştur. Bu nedenle H2 hipotezi kabul edilmiştir. Algılanan önem, BT çalışanlarının siber hijyenini pozitif yönde etkilemektedir.

H3 hipotezi ile *yanıt maliyetinin, BT çalışanlarının siber hijyen davranışsal niyetini olumsuz yönde etkileyeceği* ifade edilmiştir. Bu hipotezin, 0,010 anlamlılık düzeyi ile, 2,583 t değeri ile ve -0,096 β katsayısı ile anlamlı olduğu ortaya koyulmuştur. Bu nedenle H3 hipotezi kabul edilmiştir. Yanıt maliyeti, BT çalışanlarının siber hijyenini negatif olarak etkilemektedir.

H4 hipotezi ile *yanıt yeterliliğinin, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği* ifade edilmiştir. Bu hipotezin, 0,000 anlamlılık düzeyi, 3,610 t değeri ve -0,142 β katsayısı ile anlamlı olduğu ortaya koyulmuştur. Yanıt yeterliliği, BT çalışanlarının siber hijyenini negatif olarak etkilemektedir.

H5 hipotezi ile *öz yeterliliğin, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği* ifade edilmiştir. Bu hipotezin, 0,000 anlamlılık düzeyi, 6,685 t değeri ve 0,354 β katsayısı ile anlamlı olduğu ortaya koyulmuştur. Bu nedenle H5 hipotezi kabul edilmiştir. Öz yeterlilik, BT çalışanlarının siber hijyenini pozitif olarak etkilemektedir.

H6 hipotezi ile *öznel normların, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği* ifade edilmiştir. Bu hipotezin, 0,848 anlamlılık düzeyi, 0,192 t değeri ve 0,010 β katsayısı ile anlamlı olmadığı ortaya koyulmuştur. Bu nedenle H6

hipotezi reddedilmiştir. Siber hijyen üzerinde öznel normların bir etkisinin olmadığı anlaşılmıştır.

H7 hipotezi ile güvenlik alışkanlıklarının, *BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği ifade edilmiştir*. Bu hipotezin, 0,000 anlamlılık düzeyi, 4,834 t değeri ve 0,268 β katsayısı ile anlamlı olduğu ortaya koyulmuştur. Bu nedenle H7 hipotezi kabul edilmiştir. Güvenlik alışkanlıkları, BT çalışanlarının siber hijyenini pozitif olarak etkilemektedir.

H8 hipotezi ile bilgi güvenliği politikasına tutumun, *BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği ifade edilmiştir*. Bu hipotezin, 0,216 anlamlılık düzeyi, 1,239 t değeri ve 0,065 β katsayısı ile anlamlı olmadığı ortaya koyulmuştur. Bu nedenle H8 hipotezi reddedilmiştir. Siber hijyen üzerinde bilgi güvenliği politikasına olan tutumun önemli bir etkisinin olmadığı anlaşılmıştır.

Sonuç olarak sekiz hipotezden beşi desteklenmiş olup üç hipotez desteklenmemiştir. Bu bilgiler doğrultusunda alışkanlıkların ($\beta=0,268$; $p<0,001$), algılanan önemin ($\beta=0,134$; $p<0,05$), yanıt maliyetinin ($\beta=-0,096$; $p<0,05$), yanıt yeterliliğinin ($\beta=-0,142$, $p<0,05$), öz yeterliliğin ($\beta=0,354$; $p<0,001$) siber hijyen davranışsal niyetini etkilediği görülmüştür. Bilgi güvenliği politikasına tutum, algılanan güvenlik açığının ve öznel normlar faktörlerinin BT çalışanlarının siber hijyen davranışsal niyeti üzerinde anlamlı etkisi bulunamamıştır.

Çalışma kapsamında, önerilen modelin eldeki veriye ne kadar uygun olduğunu gösteren model uyum değerleri incelenmiştir. YEM modellerinde araştırma kapsamında test edilen modelin toplanan veri ile desteklenip desteklenmediğine uyum iyiliği indekslerine bakılarak karar verilmektedir.

Tablo 21

Uyum İndeksleri

Uyum İndeksleri	Değerler
SRMR	0,057
Chi-square	3086,542
NFI	0,800

YEM uygulamalarında yaygın olarak kullanılan birkaç uyum indeksleri vardır. Bunlardan biri de SRMR değeridir. Araştırmacılar SRMR değerinin 0'a yaklaşması mükemmel

uyuma, 1'e yaklaşması ise kötü uyuma işaretidir. SRMR değerinin 0,08'in altında veya 0,05'in altında olması yeterli görülmektedir (Gürbüz, 2021, s. 38). *Tablo 21* incelendiğinde SRMR değerinin eşik değer olan 0,08'in altında olduğu görülmektedir.

4.6. Uzaktan ve Hibrit Çalışanların Hipotez Testleri

Araştırma amacı kapsamında uzaktan ve hibrit şeklinde çalışan BT uzmanlarının siber hijyenini etkileyen faktörlerin detaylı incelenebilmesi adına iki grup için ayrı ayrı hipotez testleri gerçekleştirilmiştir. *Tablo 22* uzaktan çalışan BT uzmanlarına ait PLS analizinden oluşturulan yol katsayılarını, t-istatistiğini ve p anlamlılık durumunu göstermektedir. *Tablo 23* hibrit şeklinde çalışan BT uzmanlarına ait PLS analizinden oluşturulan yol katsayılarını, t-istatistiğini ve p anlamlılık durumunu göstermektedir. Ayrıca test edilen hipotezlerin kabul ve ret durumları da *Tablo 24*'de sunulmuştur. İlk olarak, uzaktan çalışan BT uzmanlarına ait bulgular bir bütün olarak değerlendirildiğinde Hipotez 4, Hipotez 5 ve Hipotez 7 desteklenmiştir. *Tablo 22* 'deki bilgiler doğrultusunda hipotez testleri yorumlanmıştır.

H1 hipotezi ile *algılanan güvenlik açığının, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği* ifade edilmiştir. Bu hipotezin, 0,364 anlamlılık düzeyi, 0,348 t değeri ve 0,030 β katsayısı ile anlamlı olmadığı ortaya koyulmuştur. Bu nedenle H1 hipotezi reddedilmiştir. Uzaktan çalışan BT uzmanları için algılanan güvenlik açığının siber hijyen üzerinde bir etkisi bulunmamaktadır.

H2 hipotezi ile *algılanan önemin, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği* ifade edilmiştir. Bu hipotezin, 0,062 anlamlılık düzeyi, 1,535 t değeri ve 0,090 β katsayısı ile anlamlı olmadığı ortaya koyulmuştur. Bu nedenle H2 hipotezi reddedilmiştir. Algılanan önem, uzaktan çalışan BT uzmanlarının siber hijyenini etkilememektedir.

H3 hipotezi ile *yanıt maliyetinin, BT çalışanlarının siber hijyen davranışsal niyetini olumsuz yönde etkileyeceği* ifade edilmiştir. Bu hipotezin, 0,103 anlamlılık düzeyi, 1,265 t değeri ve -0,077 β katsayısı ile anlamlı olmadığı ortaya koyulmuştur. Bu nedenle H3 hipotezi reddedilmiştir. Yanıt maliyeti, uzaktan çalışan BT uzmanlarının siber hijyenini etkilememektedir.

H4 hipotezi ile *yanıt yeterliliğinin, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği* ifade edilmiştir. Bu hipotezin, 0,028 anlamlılık düzeyi, 1,909 t

değeri ve -0,133 β katsayısı ile anlamlı olduğu ortaya koyulmuştur. Bu nedenle H4 hipotezi kabul edilmiştir. Yanıt yeterliliği, uzaktan çalışan BT uzmanlarının siber hijyenini negatif olarak etkilemektedir.

H5 hipotezi ile öz yeterliliğin, *BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği ifade edilmiştir*. Bu hipotezin, 0,000 anlamlılık düzeyi, 3,592 t değeri ve 0,308 β katsayısı ile anlamlı olduğu ortaya koyulmuştur. Bu nedenle H5 hipotezi kabul edilmiştir. Öz yeterlilik, uzaktan çalışan BT uzmanlarının siber hijyenini pozitif olarak etkilemektedir.

H6 hipotezi ile özne normların, *BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği ifade edilmiştir*. Bu hipotezin, 0,348 anlamlılık düzeyi, 0,392 t değeri ve 0,032 β katsayısı ile anlamlı olmadığı ortaya koyulmuştur. Bu nedenle H6 hipotezi reddedilmiştir. Özne normlar, uzaktan çalışan BT uzmanlarının siber hijyenini etkilememektedir.

H7 hipotezi ile güvenlik alışkanlıklarının, *BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği ifade edilmiştir*. Bu hipotezin, 0,000 anlamlılık düzeyi, 4,603 t değeri ve 0,414 β katsayısı ile anlamlı olduğu ortaya koyulmuştur. Bu nedenle H7 hipotezi kabul edilmiştir. Güvenlik alışkanlıkları, uzaktan çalışan BT uzmanlarının siber hijyenini pozitif olarak etkilemektedir.

H8 hipotezi ile bilgi güvenliği politikasına tutumun, *BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği ifade edilmiştir*. Bu hipotezin, 0,447 anlamlılık düzeyi, 0,133 t değeri ve -0,012 β katsayısı ile anlamlı olmadığı ortaya koyulmuştur. Bu nedenle H8 hipotezi reddedilmiştir. Bilgi güvenliği politikasına tutum, uzaktan çalışan BT uzmanlarının siber hijyenini etkilememektedir.

Sonuç olarak uzaktan çalışan BT uzmanları için sekiz hipotezden üç hipotez desteklenmiş olup beş hipotez desteklenmemiştir. Bu bilgiler doğrultusunda, alışkanlıkların ($\beta=0,414$; $p<0,001$), yanıt yeterliliğinin ($\beta=-0,133$; $p<0,05$), öz yeterliliğin ($\beta=0,308$; $p<0,05$) uzaktan çalışan BT uzmanlarının siber hijyen davranışsal niyetini etkilediği görülmüştür. Bilgi güvenliği politikasına tutum, algılanan güvenlik açığının, algılanan önem, yanıt maliyeti ve özne normlar faktörlerinin uzaktan çalışan BT uzmanlarının siber hijyen davranışsal niyeti üzerinde anlamlı etkisi bulunamamıştır.

Tablo 22*Uzaktan Çalışanların Yol Analizi Sonuçları*

Hipotez	Standardize β	t Değeri	P	Sonuç
H1 Algılanan Güvenlik Açığı-> CHBI	0,030	0,348	0,364	Ret
H2 Algılanan Önem-> CHBI	0,125	1,535	0,062	Ret
H3 Yanıt Maliyeti-> CHBI	-0,077	1,265	0,103	Ret
H4 Yanıt Yeterliliği-> CHBI	-0,133	1,909	0,028	Kabul
H5 Öz Yeterlilik-> CHBI	0,308	3,592	0,000	Kabul
H6 Öznel Normlar-> CHBI	0,032	0,392	0,348	Ret
H7 Alışkanlıklar-> CHBI	0,414	4,603	0,000	Kabul
H8 Bilgi Güvenliği Politikasına Tutum-> CHBI	-0,012	0,133	0,447	Ret

Araştırma amacı kapsamında hibrit şeklinde çalışan BT uzmanlarının siber hijyenini etkileyen faktörlerin detaylı incelenebilmesi adına hipotez testleri gerçekleştirilmiştir. *Tablo 23* hibrit şeklinde çalışan BT uzmanlarına ait PLS analizinden oluşturulan yol katsayılarını, t-istatistiğini ve p anlamlılık durumunu göstermektedir. Hibrit şeklinde çalışan BT uzmanlarına ait bulgular bir bütün olarak değerlendirildiğinde Hipotez 2, Hipotez 3, Hipotez 4, Hipotez 5 ve Hipotez 8 desteklenmiştir

Araştırma kapsamında önerilen hipotezler elde edilen bulgularla birlikte değerlendirilmiştir. H1 hipotezi ile *algılanan güvenlik açığının, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği* ifade edilmiştir. Bu hipotezin, 0,051 anlamlılık düzeyi 1,635 t değeri ve 0,126 β katsayısı ile anlamlı olmadığı ortaya koyulmuştur. Bu nedenle H1 hipotezi reddedilmiştir. Hibrit şeklinde çalışan BT uzmanları için algılanan güvenlik açığının siber hijyen üzerinde bir etkisi bulunmamaktadır.

H2 hipotezi ile *algılanan önemin, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği* ifade edilmiştir. Bu hipotezin, 0,031 anlamlılık düzeyi, 1,535 t değeri ve 0,148 β katsayısı anlamlı olduğu ortaya koyulmuştur. Bu nedenle H2 hipotezi kabul edilmiştir. Algılanan önem, hibrit çalışan BT uzmanlarının siber hijyenini pozitif olarak etkilemektedir.

H3 hipotezi ile *yanıt maliyetinin, BT çalışanlarının siber hijyen davranışsal niyetini olumsuz yönde etkileyeceği ifade edilmiştir*. Bu hipotezin, 0,034 anlamlılık düzeyi, 1,819 t değeri ve -0,095 β katsayısı ile anlamlı olduğu ortaya koyulmuştur. Bu nedenle H3 hipotezi kabul edilmiştir. Yanıt maliyeti, hibrit şeklinde çalışan BT uzmanlarının siber hijyenini negatif olarak etkilemektedir.

H4 hipotezi ile *yanıt yeterliliğinin, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği ifade edilmiştir*. Bu hipotezin, 0,000 anlamlılık düzeyi, 3,487 t değeri ve -0,190 β katsayısı ile anlamlı olduğu ortaya koyulmuştur. Bu nedenle H4 hipotezi kabul edilmiştir. Yanıt yeterliliği, hibrit şeklinde çalışan BT uzmanlarının siber hijyenini negatif olarak etkilemektedir.

H5 hipotezi ile *öz yeterliliğin, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği ifade edilmiştir*. Bu hipotezin, 0,000 anlamlılık düzeyi, 5,767 t değeri ve 0,464 β katsayısı ile anlamlı olduğu ortaya koyulmuştur. Bu nedenle H5 hipotezi kabul edilmiştir. Öz yeterlilik, hibrit şeklinde çalışan BT uzmanlarının siber hijyenini pozitif olarak etkilemektedir.

H6 hipotezi ile *özel normların, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği ifade edilmiştir*. Bu hipotezin, 0,447 anlamlılık düzeyi, 0,132 t değeri ve 0,011 β katsayısı ile anlamlı olmadığı ortaya koyulmuştur. Bu nedenle H6 hipotezi reddedilmiştir. Özel normlar, hibrit şeklinde çalışan BT uzmanlarının siber hijyenini etkilememektedir.

H7 hipotezi ile *güvenlik alışkanlıklarının, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği ifade edilmiştir*. Bu hipotezin, 0,080 anlamlılık düzeyi, 1,402 t değeri ve 0,117 β katsayısı ile anlamlı olmadığı ortaya koyulmuştur. Bu nedenle H7 hipotezi reddedilmiştir. Güvenlik alışkanlıkları, uzaktan çalışan BT uzmanlarının siber hijyenini etkilememektedir.

H8 hipotezi ile *bilgi güvenliği politikasına tutumun, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkileyeceği ifade edilmiştir*. Bu hipotezin, 0,045 anlamlılık düzeyi, 1,696 t değeri ve 0,133 β katsayısı ile anlamlı olduğu ortaya koyulmuştur. Bu nedenle H8 hipotezi kabul edilmiştir. Bilgi güvenliği politikasına tutum, hibrit şeklinde çalışan BT uzmanlarının siber hijyenini pozitif yönde etkilemektedir.

Sonuç olarak uzaktan çalışan BT uzmanları için sekiz hipotezden beş hipotez desteklenmiş olup üç hipotez desteklenmemiştir. Bu bilgiler doğrultusunda, algılanan

önemin ($\beta = 0,148$; $p < 0,05$), yanıt maliyetinin ($\beta = -0,095$; $p < 0,05$), yanıt yeterliliğinin ($\beta = -0,190$, $p < 0,001$), öz yeterliliğin ($\beta = 0,464$; $p < 0,001$) ve bilgi güvenliği politikasına tutumun ($\beta = 0,133$, $p < 0,05$) hibrit şeklinde çalışan BT uzmanlarının siber hijyen davranışsal niyetini etkilediği görülmüştür. Algılanan güvenlik açığı, alışkanlıklar ve öznel normlar faktörlerinin hibrit şeklinde çalışan BT uzmanlarının siber hijyen davranışsal niyeti üzerinde anlamlı etkisi bulunamamıştır.

Tablo 23

Hibrit Şeklinde Çalışanların Yol Analizi Sonuçları

Hipotez	Standardize β	t Değeri	P	Sonuç
H1 Algılanan Güvenlik Açığı-> CHBI	0,126	1,635	0,051	Ret
H2 Algılanan Önem-> CHBI	0,148	1,535	0,031	Kabul
H3 Yanıt Maliyeti-> CHBI	-0,095	1,819	0,034	Kabul
H4 Yanıt Yeterliliği-> CHBI	-0,190	3,487	0,000	Kabul
H5 Öz Yeterlilik-> CHBI	0,464	5,767	0,000	Kabul
H6 Öznel Normlar-> CHBI	0,011	0,132	0,447	Ret
H7 Alışkanlıklar-> CHBI	0,117	1,402	0,080	Ret
H8 Bilgi Güvenliği Politikasına Tutum-> CHBI	0,133	1,696	0,045	Kabul

Uzaktan ve hibrit şeklinde çalışan BT uzmanlarıyla ilgili bilgiler *Tablo 24'* de karşılaştırılmalı olarak gösterilmektedir. Analizler neticesinde her iki grubu da anlamlı olarak etkileyen faktörler yanıt yeterliliği ($\beta = -0,133$; $p = 0,028$ - $\beta = -0,190$; $p = 0,000$) ve öz yeterlilik ($\beta = 0,308$; $p = 0,000$ - $\beta = 0,464$; $p = 0,000$) olmuştur. Her iki grupta anlamsız çıkan faktörler algılanan güvenlik açığı ($\beta = 0,030$; $p = 0,364$ - $\beta = 0,126$; $p = 0,051$) ve öznel normlardır ($\beta = 0,032$; $p = 0,348$ - $\beta = 0,011$; $p = 0,447$). Güvenlik alışkanlıkları faktörü uzaktan çalışan BT uzmanları için anlamlı ($\beta = 0,414$; $p = 0,000$) bir faktör olarak gözükmekte iken hibrit şeklinde çalışan BT uzmanları için anlamsız ($\beta = 0,117$; $p = 0,080$) bir faktör olarak gözükmektedir. Ayrıca bilgi güvenliğine politikasına tutum faktörü de uzaktan çalışan BT uzmanları için anlamsız ($\beta = -0,012$; $p = 0,447$), hibrit şeklinde çalışan BT uzmanları için anlamlı ($\beta = 0,133$; $p = 0,045$) faktör olarak çıkmıştır. Benzer şekilde yanıt maliyeti uzaktan çalışan BT uzmanları için anlamsız ($\beta = -0,077$; $p = 0,103$) bir faktör iken hibrit şeklinde çalışan BT uzmanları için anlamlı ($\beta = -0,095$; $p = 0,034$) bir faktör olarak ortaya çıkmıştır. Son olarak algılanan önem uzaktan çalışan BT uzmanları için

anlamsız ($\beta=0,125$; $p=0,062$) iken hibrit şeklinde çalışan BT uzmanları için anlamlı ($\beta=0,148$; $p=0,031$) bir faktör olarak ortaya çıkmıştır.



Tablo 24*Uzaktan ve Hibrit Çalışanların Karşılaştırılmalı Gösterimi*

	Standardize β (Hibrit)	Standardize β (Uzaktan)	Ort. (Hibrit)	Ort. (Uzaktan)	Sd. Sapma (Hibrit)	Sd. Sapma (Uzaktan)	t değeri (Hibrit)	t değeri (Uzaktan)	p değeri (Hibrit)	p değeri (Uzaktan)
HBT -> CHBI	0.117	0.414	0.115	0.417	0.084	0.090	1.402	4.603	0.080	0.000
ISP -> CHBI	0.133	-0.012	0.139	-0.016	0.078	0.089	1.696	0.133	0.045	0.447
PS -> CHBI	0.148	0.125	0.152	0.139	0.079	0.081	1.865	1.535	0.031	0.062
PV -> CHBI	0.126	0.030	0.137	0.042	0.077	0.087	1.635	0.348	0.051	0.364
RC -> CHBI	-0.095	-0.077	-0.093	-0.089	0.052	0.061	1.819	1.265	0.034	0.103
RE -> CHBI	-0.190	-0.133	-0.184	-0.115	0.055	0.070	3.487	1.909	0.000	0.028
SE -> CHBI	0.464	0.308	0.466	0.299	0.080	0.086	5.769	3.592	0.000	0.000
SN -> CHBI	0.011	0.032	0.001	0.025	0.080	0.082	0.132	0.392	0.447	0.348

Not:HBT(Alışkanlıklar), ISP (Bilgi Güvenliği Politikasına Tutum), PS (Algılanan Önem), PV(Algılanan Güvenlik Açığı), RC (Yanıt Maliyeti), RE (Yanıt Yeterliliği), SE (Öz Yeterlilik), SN (Öznel Normlar), CHBI (Siber Hijyen Davranışsal Niyet)

4.7. Bulguların Kuramsal Temel Çerçevesinde Değerlendirilmesi

Bu bölümde analizler neticesinde elde edilen bulguların literatür odaklı tartışması araştırma kapsamında önerilen hipotezlerin genel değerlendirmesi yapılacaktır. Araştırma bulguları, siber hijyen davranışının bazı ilginç ve beklenmedik yönlerini ortaya çıkarmıştır. Güvenlik davranışına ilişkin araştırmaların çoğunluğunun sıradan kurumsal çalışanlar üzerinden yürütüldüğü göz önüne alındığında, onlar için geçerli olan BT çalışanları için geçerli olmayacaktır. Kurum içindeki bilgi sistemleri ile ilgili olarak rolleri ve sorumlulukları dikkate alındığında bazı bulguların literatürdeki çalışmalardan farklılaşmasını açıklamak için geçerli bir sebeptir.

Araştırma bulguları, algılanan güvenlik açığı dışında tüm KMT değişkenlerinin siber güvenlik davranışını önemli ölçüde etkilediğini göstermiştir. Rogers (1975)'in KMT modelinde önerdiği algılanan önem, yanıt maliyeti, yanıt yeterliliği ve öz yeterlilik BT çalışanlarının güvenlik davranışı belirlemede önemli rol oynamaktadır. Fakat algılanan güvenlik açığı BT çalışanlarının güvenlik davranışında rol oynamadığı tespit edilmiştir. Literatürde algılanan güvenlik açığı genellikle kurumsal ortamdaki güvenlik davranışlarını etkilediği bulunmasına rağmen bu konuda tartışmaları zıt bulgularda mevcuttur. Bazı araştırmalarda algılanan güvenlik açığının güvenlik davranışı üzerinde olumlu etkisi bulunmuşken (Claar ve Johnson, 2012; Ifinedo, 2012; Liang ve Xue, 2010a; M. Siponen vd., 2014; Workman vd., 2008), bazı araştırmalarda ise algılanan güvenlik açığının güvenlik davranışı üzerinde etkisinin olmadığı bulunmuştur (Blythe ve Coventry, 2018; Crossler ve Bélanger, 2014; R. E. Crossler, 2010; Hanus ve Wu, 2016; Sulaiman vd., 2022; Tsai vd., 2016; Yoon vd., 2012). BT çalışanları üzerine yapılan başka bir araştırmada ise, algılanan güvenlik açığı ile masaüstü güvenlik davranış arasında anlamlı fakat olumsuz bir ilişki olduğu bulunmuştur (Torten vd., 2018). Karışık bulguların olmasının nedeni, güvenlik açığının, ortamlarına bağlı olarak kullanıcılar için farklı anlamlara ifade etmesi olabilmektedir (Dang-Pham ve Pittayachawan, 2015).

Algılanan güvenlik açığı bir kişinin tehdit riski altında olabileceğine inanıp inanmadığının bir değerlendirmesidir (Yoon vd., 2012). Algılanan güvenlik açığının bu çalışma kapsamında önemsiz çıkmasının nedeni çalışma örnekleminde yer alan BT çalışanlarının siber güvenlik tehdit algısının tam oluşmadığı veya bu tehditlerin

gerçekleşme ihtimal ve olası zararları hakkında farkındalık sahibi oldukları olabilir. BT çalışanlarının otomatik olarak her zaman meydana gelebilecek olası en şiddetli olaya karşı tetikte olmaya ve onunla mücadele etmeye hazır olmaya meyilli olacağından bu değişkenin etkisinin büyük olmayacağı söylenebilir.

İkinci olarak bu çalışmada algılanan önemin, BT çalışanlarının siber hijyen davranışsal niyetini pozitif olarak etkilediği bulunmuştur. Literatürde algılanan önemin siber güvenlik davranışları üzerindeki etkisini bildiren birçok çalışma vardır (Bulgurcu vd., 2010; Burns vd., 2017; Posey vd., 2016). Marett vd. (2011) tarafından yapılan bir çalışmada, algılanan önemin güvenlik davranışı üzerinde olumlu bir etkisi olduğu bulunmuştur. Benzer şekilde, başka bir çalışmada algılanan önemin web sayfalarıyla ilgili güvenlik davranışları üzerinde güçlü bir etkisi olduğunu bulunmuştur (Abraham ve Chengalur-Smith, 2019). Herath ve Rao (2009a) tarafından yapılan çalışmada, algılanan önemin çalışanların bilgi sistemleri güvenlik politikalarını benimseme niyeti üzerinde anlamlı bir etkiye sahip olduğunu bulunmuştur. BT profesyonellerine yapılan bir çalışmada algılanan önem ile masaüstü güvenlik davranışları arasında istatistiksel olarak anlamlı bir ilişkinin olmadığı tespit edilmiştir (Torten vd., 2018). Bu çalışmada siber hijyen odaklı olduğu için algılanan önem etkili bir faktör olarak ortaya çıkmıştır.

Üçüncü olarak, bu çalışmada yanıt maliyetinin, BT çalışanlarının siber hijyen davranışsal niyetini olumsuz yönde etkilediği bulunmuştur. Bu sonuç literatürdeki çalışmalarla uyumludur (Ifinedo, 2012; Johnston ve Warkentin, 2010; Vance vd., 2012; Workman vd., 2008). Örneğin Ma (2022) tarafından BT çalışanlarına yapılan çalışmada yanıt maliyetinin anlamlı etkisi bulunmuştur. Fakat literatürdeki bazı çalışmalarda yanıt maliyetinin bilgi güvenliği politikasına uymaya yönelik davranışsal niyet üzerinde anlamlı bir etkisinin olmadığı bulunmuştur (Sharma ve Aparicio, 2022). Literatürde BT çalışanları üzerine yapılan başka bir çalışmada yanıt maliyetinin bilgi güvenliği davranışsal niyetini etkilemediği bulunmuştur (Hooper ve Blunt, 2019)

Dördüncü olarak, bu çalışma örnekleme kapsamında yanıt yeterliliğinin, BT çalışanlarının siber hijyen davranışsal niyetini olumsuz yönde etkilediği bulunmuştur. Yapılan bir araştırma da ise yanıt yeterliliğinin bilgi güvenliği politikalarına uyma niyetini negatif olarak etkilediği bulunmuştur (Vance vd., 2012). Siponen vd. (2021) tarafından yapılan bir çalışmada ise yanıt yeterliliğinin bilgi güvenliği politikalarına uyma niyetini

etkilemediği bulunmuştur. Tsai vd.. (2016) tarafından yapılan araştırmada ise algılanan önemin bilgisayar kullanıcılarının güvenlik niyetleri üzerinde olumsuz bir etkiye sahip olduğunu bulunmuştur. BT çalışanları üzerine yapılan başka bir araştırmada yanıt yeterliliğinin bilgi güvenliği davranışsal niyetini etkilemediği bulunmuştur (Hooper ve Blunt, 2019).

Beşinci olarak, bu çalışma örneklemini kapsamında öz yeterliliğin, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkilediği bulunmuştur. Literatürde öz yeterlilik ile koruyucu güvenlik davranışı gerçekleştirme niyeti veya bilgi güvenliği politikasına uyum niyeti arasında pozitif ilişkiler olduğunu gösteren çok sayıda çalışma bulunmaktadır (Abraham ve Chengalur-Smith, 2019; Bulgurcu vd., 2010; Ifinedo, 2012, 2014; Pahnla vd., 2007; Siponen vd., 2014; Vance vd., 2012; Workman vd., 2008). BT çalışanları üzerine yapılan başka bir araştırmada öz yeterliliğinin bilgi güvenliği davranışsal niyetini etkilediği bulunmuştur (Hooper ve Blunt, 2019). BT çalışanlarının teknolojik yetenekleri iyi derecede olduğu için kendilerine bu konuda oldukça güven duyacaklardır ve güvenlik önlemlerini uygulama konusunda kendilerini yeterli hissedeceklerdir.

Altıncı olarak, bu çalışma örneklemini kapsamında öznel normların, BT çalışanlarının siber hijyen davranışsal niyetini etkilemediği bulunmuştur. Bu bulgu literatürdeki BT çalışanları üzerine yapılan çalışmalarla tutarlıdır (Hooper ve Blunt, 2019). Fakat kurumsal çalışanlar üzerinden yapılan çalışmalarda kurumsal çalışanların öznel normlardan etkilendiği bulunmuştur (Herath ve Rao, 2009b; Johnston ve Warkentin, 2010; Pahnla vd., 2007). Bu çalışmanın sonuçları kurumsal çalışanlara yapılan çalışmaların sonuçlarıyla tutarlı değildir. Bunun nedeni, BT çalışanlarının, BT ve BT güvenliği yetenekleri konusunda, kendilerini tavsiyede bulunan diğer kişilerden daha bilgili düşündüklerinden ve kendilerine daha çok güvenmelerinden kaynaklı olabilir. Sonuç olarak, siber güvenlik önlemleri konusunda başkalarının, BT çalışanlarının siber hijyen davranışsal niyetleri üzerinde etkisi yoktur.

Yedinci olarak, güvenlik alışkanlıklarının, BT çalışanlarının siber hijyen davranışsal niyetini olumlu yönde etkilediği bulunmuştur. Bu sonuç literatürdeki çalışmalarla uyumludur. Literatürde güvenlik davranışı ile bilgi güvenliği politikasına uyum niyetleri arasında pozitif bir ilişkinin olduğu bulunmuştur (Moody vd., 2018; Pahnla vd., 2007;

Vance vd., 2012). Benzer şekilde Aigbefo vd. (2022) tarafından yapılan çalışmada, kobi çalışanlarının güvenlik davranışı niyetlerinde alışkanlıkların güçlü bir etkisi olduğu bulunmuştur ($\beta = 0.420$). Shahbaznezhad vd. (2021) tarafından yapılan bir araştırmada, çalışanların ortalama maillerine tıklama niyetini güvenlik alışkanlıklarının etkilediği bulunmuştur.

Sekizinci olarak, bilgi güvenliği politikasına tutumun, BT çalışanlarının siber hijyen davranışsal niyetini etkilemediği bulunmuştur. BT çalışanları açısından siber hijyen üzerinde bilgi güvenliği politikasına olan tutumun önemli bir etkisinin olmadığı görülmüştür. Siponen vd. (2014), tutumun kurumsal bilgi güvenliği politikalarına uyumla olumlu yönde ilişkili olduğunu ve çalışanların güvenlik politikalarına uyma niyetini etkilediğini bulmuştur. Ifinedo (2012) tarafından yapılan çalışmada ise kurumsal çalışanların bilgi güvenliği politikalarına yönelik tutumun bilgi güvenliği politikalarına uyma davranışsal niyetini etkilediği bulunmuştur. Bu çalışmanın sonuçları literatürdeki çalışmalarla uyumlu olmamasının nedeni, bilgi güvenliği politikalarına tutumun güvenlik niyetleri üzerindeki etkisi araştırmasıdır. Çalışma kapsamında bu etkinin anlamsız çıkmasının nedeni bilgi güvenliği politikalarının yetersiz olması veya güncel olmaması olabilir. Ayrıca, BT çalışanlarının güvenlik konusunda diğer çalışanlardan daha bilgili olmaları olabilir. Güvenlik konusuna öz yeterliliklerinin yüksek olan BT çalışanları kendi yeteneklerine veya deneyimlerine güvendiklerinden kendilerini politikalara uymak zorunda hissetmeyebilirler. Başka bir sebep ise, bazı bilgi güvenliği politikalarının aşırı güvenlik önlemleri nedeniyle çalışanların iş akışını engelleyebilmektedir. Bu durumda BT çalışanları verimliliklerini artırmak için bilgi güvenliği politikaları ihmal eder veya gereksiz bir zorunluluk olarak görebilirler. Kurum içinde üst yönetimin bilgi güvenliği politikalarına yeterince önem vermemesi ve farkındalık oluşturmak adına gerekli adımları atmaması da sebeplerden biridir.

Özetle, uzaktan veya hibrit şeklinde çalışan BT uzmanlarının siber hijyen davranışsal niyetleri, algılanan önem, yanıt maliyeti, yanıt yeterliliği, öz yeterlilik ve güvenlik alışkanlıkları faktörlerinden etkilenmektedir. Algılanan güvenlik açığı, öznel normlar ve bilgi güvenliği politikalarına tutum faktörlerinden ise etkilenmemektedir. Söz konusu bu bulgular sadece uzaktan veya hibrit şeklinde çalışan BT uzmanları için geçerlidir. Ofisten çalışan BT çalışanları için aynı faktörler geçerli olmayabilir. Farklı gruplar farklı güvenlik

davranışları sergileyebilmektedir. Bunun nedeni farklı rol değerlerinin olması ve çalışma ortamının farklılıklarından kaynaklanmaktadır.



SONUÇ VE ÖNERİLER

Bu çalışma içinde bulunduğumuz zaman diliminde kurumlar için vazgeçilmez bir çalışma grubu olan BT çalışanlarına odaklanmaktadır. Kurumların bilgi teknolojilerine bağımlı olduğu bu çağda, dijital varlıkları koruyabilmek adına BT çalışanlarına ihtiyaç duymaktadır. BT çalışanları kullanıcı adı ve parola, kimlik bilgileri, ağa giriş bilgileri, sisteme giriş bilgileri gibi bilgilere olan yetkisi düşünüldüğünde kurumlar için en kritik çalışan grubunu oluşturmaktadır. Bu nedenle, BT çalışanları diğer çalışan gruplarına kıyasla daha önemlidir. Kurum bilgilerinin güvende kalması için BT çalışanlarının siber hijyen farkındalığının artırılması gerekmektedir. Bu araştırma, kurumlar için kritik öneme sahip olan BT çalışanlarına odaklanmıştır.

Çalışmada, BT çalışanlarının bilgi ve bilgisayar güvenliği davranışsal niyetlerini araştırılmıştır. Teorik olarak koruma motivasyon teorisi, mantıklı eylem teorisi ve alışkanlık teorilerinin bir kombinasyonu ile uzaktan veya hibrit şeklinde çalışan BT uzmanlarının siber hijyen davranışsal niyetlerini hangi faktörlerin etkilediğini araştırılmıştır. BT çalışanlarının siber hijyen davranışsal niyetlerinde hangi faktörlerin etkili rol oynadığı ve hangi faktörlerin önemli olmadığı belirlenerek araştırma sorularına cevap aranmıştır.

Araştırma kapsamında ele alınacak temel araştırma problemi “Koruma motivasyon teorisi faktörleri, mantıklı eylem teorisi faktörleri ve alışkanlıklar teorisi faktörleri bilişim sektöründe uzaktan veya hibrit çalışanların siber hijyen davranışlarını nasıl etkiler ?” olarak belirlenmiştir. Bu temel araştırma problemini cevaplamak adına aşağıdaki alt sorulara cevap aranmıştır.

1) Koruma motivasyon teorisi faktörleri BT çalışanlarının siber hijyenini nasıl etkiler?

Çalışma sonuçlarına göre BT çalışanlarının siber hijyenini etkileyen temel motivasyonel faktörler algılanan önem, yanıt maliyeti, yanıt yeterliliği ve öz yeterlilik olduğu tespit edilmiştir. Ayrıca siber hijyeni etkilemeyen motivasyonel faktörler ise, algılanan güvenlik açığı olduğu tespit edilmiştir.

2) BT çalışanlarının güvenlik alışkanlıkları siber hijyeni nasıl etkilemektedir?

Çalışma sonuçlarına göre BT çalışanlarının siber hijyenini güvenlik alışkanlıklarının olumlu yönde etkilediği tespit edilmiştir. Standardize beta katsayısı incelendiğinde güvenlik alışkanlıklarının siber hijyen davranışsal niyeti üzerinde $\beta = 0,268$ düzeyinde bir etkiye sahip olduğu görülmektedir.

3) Çalışma tipine (uzaktan ve hibrit) göre BT çalışanlarının siber hijyenini etkileyen faktörler nasıl farklılık gösterir?

Çalışma sonuçlarına göre uzaktan çalışan BT uzmanlarının siber hijyenini etkileyen faktörler yanıt yeterliliği, öz yeterlilik ve güvenlik alışkanlıkları olduğu tespit edilmiştir. Ayrıca uzaktan çalışan BT uzmanlarının siber hijyeni etkilemeyen faktörler ise, algılanan güvenlik açığı, algılanan önem, yanıt maliyeti, öznel normlar ve bilgi güvenliği politikalarına tutum olmuştur.

Hibrit şeklinde çalışan BT uzmanlarının siber hijyenini etkileyen faktörler algılanan önem, yanıt maliyeti, yanıt yeterliliği, öz yeterlilik ve bilgi güvenliği politikalarına tutum olduğu tespit edilmiştir. Ayrıca hibrit şeklinde çalışan BT uzmanlarının siber hijyeni etkilemeyen faktörler ise, algılanan güvenlik açığı, öznel normlar ve güvenlik alışkanlıkları olmuştur.

Temel Araştırma Problemi: “Koruma motivasyon teorisi faktörleri, mantıklı eylem teorisi faktörleri ve alışkanlıklar teorisi faktörleri bilişim sektöründe uzaktan veya hibrit çalışanların siber hijyen davranışlarını nasıl etkiler ?”

BT çalışanlarının siber hijyenini etkileyen temel faktörler algılanan önem, yanıt maliyeti, yanıt yeterliliği, öz yeterlilik ve güvenlik alışkanlıkları olduğu tespit edilmiştir. Algılanan güvenlik açığı, öznel normlar ve bilgi güvenliği politikaları ise BT çalışanlarının siber hijyen davranışsal niyetini etkilemediği tespit edilmiştir.

Algılanan önemin, BT çalışanlarının siber hijyen davranışsal niyetini pozitif olarak etkilediği bulunmuştur. Çalışanlar siber güvenlik olaylarının kurum için önemli olduğunu ve ciddi derecede zararlara neden olacağını öğrendiğinde güvenlik önlemleri uygulamada daha istekli olacaktırlar. Örneğin, kuruma siber saldırı gerçekleştiğinde bu ihalilin yaşam döngüsünün, tespit edilip kontrol altına alınmasına kadar geçen sürenin 277 gün olduğu

tespit edilmiştir. Ayrıca, bir güvenlik ihlalinin kuruma maliyetinin 4,45 milyon dolar olduğu ortaya çıkarılmıştır (IBM, 2023). Bu nedenle kurumlara siber saldırı yaşandığında kuruma ne kadar maliyetli olabileceği ve saldırı sonrası eski iş performansına dönmenin ne kadar uzun süreceği olası hikaye senaryoları ile siber güvenlik farkındalık programlarına dahil edilmesi önerilmektedir.

Yanıt maliyetinin ve yanıt yeterliliğinin BT çalışanlarının siber hijyen davranışsal niyetini negatif olarak etkilediği bulunmuştur. Güvenlik önlemlerinin fazla iş yükü ve zaman alan uygulamalar olduğu algısında olan BT çalışanlarının siber hijyen davranışı gerçekleştirme olasılıkları daha düşük olacaktır. Diğer taraftan kurum tarafından alınan mevcut önlemlerin BT çalışanları tarafından yeterli görülmesi algısı siber hijyen davranışını gerçekleştirme ihtimallerini düşürecektir. BT çalışanları kurum zaten gerekli önlemleri alıyor hissine kapılarak güvenlik davranışlarını azalatabilir. BT çalışanları kurumların almış olduğu teknolojik önlemlere aşırı güvenmektedir. Bu nedenle kurum tarafından alınan önlemler olsa da son kullanıcının siber hijyen davranışları olmadan siber güvenlikte başarılı olunamayacağı örnek olaylar üzerinden anlatılması gerekmektedir. Ek olarak, siber güvenlik önlemlerinin BT çalışanlarına fazla iş yükü getirmeyecek ve fazla zamanını almayacak şekilde tasarlanmalıdır.

Öz yeterliliğin, BT çalışanlarının siber hijyen davranışsal niyetini pozitif olarak etkilediği bulunmuştur. BT çalışanlarının teknolojik yeteneklerine oldukça güven duyacaklarına ve siber güvenlik önlemlerini uygulama yeterliliğini hissedecekleri için siber hijyeni olumlu yönde etkilemiştir. Kurumlar BT çalışanlarının öz yeterliliklerini artırdığında dolayı olarak siber hijyeni de artıracaktır. Bu nedenle, kurumlara çalışanlarının öz yeterliliklerini artırması adına siber güvenlik üzerine eğitimlerin düzenli aralıklarla verilmesi ve çalışanların desteklenmesi önerilmektedir.

Güvenlik alışkanlıkları, BT çalışanlarının siber hijyen davranışsal niyetini pozitif olarak etkilediği bulunmuştur. BT çalışanları genellikle bilgisayar bilimi veya bilgi teknolojileri gibi alanlarda eğitim aldıkları için güvenlik alışkanlıklarının olması muhtemeldir. Fakat bu tez kapsamında önemli olan güvenlik alışkanlıklarının siber hijyeni olumlu derecede etkilemesidir. Güvenlik ile ilgili kazanılan alışkanlıklar siber hijyen uygulamalarının takip edilmesi ve benimsenmesinde etkili olmaktadır. Bu noktada şirketlere BT

alıřanlarının siber hijyenini geliřtirmek iin gl gvenlik alıřkanlıklarının kazandırılması nerilmektedir.

Algılanan gvenlik aıęının, BT alıřanlarının siber hijyenini etkilemedięi bulunmuřtur. Algılanan gvenlik aıęının bu alıřma kapsamında nemsiz ıkmasının nedeni alıřma rnekleminde yer alan BT alıřanlarının siber gvenlik tehdit algısının tam oluřmadıęı veya bu tehditlerin gerekleřme ihtimal ve olası zararları hakkında farkındalık sahibi oldukları olabilir. BT alıřanlarının otomatik olarak her zaman meydana gelebilecek olası en řiddetli olaya karřı tetikte olmaya ve onunla mcadele etmeye hazır olacaęından bu deęiřkenin etkisi olmayabilir. Ayrıca, kurumların, alıřanların bilgi gvenlięini ciddiye almaması ve politikalara uymaması durumunda siber gvenlik tehditlerine maruz kalabileceklerini vurgulamaları gerekmektedir. Bu bilgilendirme siber gvenlik seminerleri ve eęitim panelleri vb. yoluyla yapılabilir.

znel normların, BT alıřanlarının siber hijyenini etkilemedięi bulunmuřtur. znel normların bu alıřma kapsamında anlamsız ıkmasının nedeni, BT alıřanlarının, BT ve BT gvenlięi yetenekleri konusunda, kendilerini tavsiyede bulunan dięer kiřilerden daha bilgili dřndklerinden ve kendilerine daha ok gvenmelerinden kaynaklı olabilir. Sonu olarak, siber gvenlik nlemleri konusunda bařkalarının, BT alıřanlarının siber hijyen davranıřsal niyetleri zerinde etkisi yoktur.

Bilgi gvenlięi politikalarına tutumun, BT alıřanlarının siber hijyenini etkilemedięi bulunmuřtur. Bunun nedeni, bilgi gvenlięi politikalarının yetersiz olması veya gncel olmaması olabilir. Ayrıca, BT alıřanlarının gvenlik konusunda dięer alıřanlardan daha bilgili olmaları olabilir. Gvenlik konusuna z yeterliliklerinin yksek olan BT alıřanları kendi yeteneklerine veya deneyimlerine gvendiklerinden kendilerini politikalara uymak zorunda hissetmeyebilirler.

Teorik ve Pratik Katkıları

Bu arařtırma, bireysel davranıřın kritik bir rol oynadıęı uzaktan ve hibrit alıřma gibi yeni ortaya ıkan alıřma tarzlarına nemli teorik ve pratik katkıları sunmaktadır. İlk olarak, uzaktan ve hibrit alıřan BT uzmanlarının siber hijyenini inceleyen alıřma olarak literatre katkı saęlamaktadır. İkinci olarak, siber hijyen davranıřları rasyonel eylemler olduęundan, alıřma siber hijyen davranıřsal niyetleri koruma motivasyon teorisi,

mantıklı eylem teorisi ve alışkanlıklar teorisinin kapsamında inceleyerek güvenilir ve geçerli bir model geliştirmiştir. Pratikte ise bu çalışma, uzaktan ve hibrit şeklinde çalışan BT uzmanlarının siber güvenlik farkındalığını artırmayı amaçlayan politika yapıcılara değerli bir rehberlik sağlayacaktır. Son olarak, yöneticilere bireysel davranışları kurumsal güvenlik politikalarıyla uyumlu hale getirme konusunda yardımcı olabilir.

Kurumlara Öneriler

Akademik çalışmaların öncelikli amacı literature katkı sağlamaktır. İkinci amacı ise değerli önerilerle uygulamaya katkı sağlamaktadır. Çalışma bulgularından hareketle kurumlar için bazı öneriler sunulmaktadır.

- 1) **Siber güvenlik kültürünün oluşturulması:** Kültür çalışan tutum ve davranışlarını şekillendireceğinden güçlü bir siber güvenlik kültürü güvenlik davranışları üzerine olumlu bir etki yaratacaktır. Siber güvenlik kültürüne sahip bir kurumda çalışmak BT çalışanlarını güvende hissettirir ve verimliliği artırır. Aynı zamanda BT çalışanları siber güvenlik konusunda tüm iş yükünün kendisinde olmadığını bildiği takdirde kurum bağlılığı ve sadakati de artacaktır. Çünkü siber güvenlik sadece BT çalışanlarına üzerine yüklenemeyecek kadar büyük bir konudur. Bu nedenle kurumlara, siber hijyen davranışlarını iyileştirmek adına siber güvenlik kültürünün oluşturulması BT çalışanlarını iş memnuniyetini sağlama noktasında önerilmektedir.
- 2) **Sürekli eğitim ve sertifikasyonlar:** BT çalışanlarının öz yeterliliklerin artırılması siber hijyen derecelerinde artıracaktır. Çalışanlara verilecek olan eğitim ve sertifikalar öz yeterliliği artıracak ve bu da siber hijyen davranışlarına iyi yönde yansıyacaktır. Siber güvenlik yeni teknolojilerin ortaya çıkmasıyla sürekli olarak gelişen ve değişen bir alandır. BT çalışanlarına güncel trendlere ve teknolojilere uygun siber güvenlik eğitim ve sertifikasyon imkanları sunmak, siber güvenlik bilgi ve becerilerini güncel tutmalarına yardımcı olacaktır. Siber saldırı olaylarını koordine etmek ve yönetmek için olay yönetimi eğitimi gibi yeni nesil araç ve tekniklerin benimsenmesini öneriyoruz. Bu faaliyetler çalışanların siber hijyen davranışlarının iyileştirilmesine yardımcı olacaktır.
- 3) **Çalışan davranışlarını ödüllendirmek:** Ödüllendirme iyi siber hijyen davranışlarının gerçekleşmesini ve sürdürülmesini sağlayabilmektedir. BT

çalışanları iyi bir güvenlik davranışı gösterdiğinde bunun ödüllendirilmesi siber hijyen davranışının tekrarlanmasını sağlayabilir. Ve bu şekilde güvenlik alışkanlıkları çalışanlara kazandırılabilir. Ödüllendirme diğer çalışanları da aynı şekilde davranmaya teşvik edebilir. Örneğin bazı kurumlar şüpheli mesajları bildiren çalışanlarına hediye çeki gibi ödüller vermektedir. Bu nedenle kurumlara iyi siber hijyen davranışlarını gerçekleştiren çalışanların ödüllendirilmesi güvenlik alışkanlıklarının kazanılması adına önerilmektedir.

- 4) **Siber güvenlik politikaları:** Siber güvenlik politikalarına uyumun, çalışanların işlerini yapmalarını engelleyen bir durum olarak değil, bir gereklilik olarak görülmesini teşvik edecek çalışma ortamı oluşturulması gerekmektedir. BS güvenlik uygulamaları ve prosedürleri BT çalışanların iş akışını yavaşlatacak düzeyde olmamalıdır. Aksi takdirde, çalışanlar siber güvenlik politikalarına bağlı kalmanın çok fazla zaman aldığı hissine kapılırsa BS politikalarına uyum sağlamayacaktır. Özellikle BT çalışanları, yeteneklerine veya önlemlerine güvenerek siber güvenlik politikalarını gereksiz bulabilir. Bu nedenle, kurumlara, siber güvenlik politikaları oluşturulurken BT çalışanlarından öneriler alınması tavsiye edilmektedir.
- 5) **İzleme ve kontrol:** BT çalışanları önemli bilgilere ve kritik sistemlere erişimi vardır. Bu nedenle siber hijyen davranışlarının zayıf olması iç güvenlik ihlallerine, veri sızıntılarına veya yetkisiz erişimlere yol açabilmektedir. Dolayısıyla yöneticilere, BT çalışanlarının davranışlarını düzenli aralıklarla izlemesi ve kontrol edilmesi önerilmektedir. Ayrıca, BT çalışanlarının sadece işlerini yapmak için ihtiyaç duydukları verilere erişimlerinin olması diğer verilere erişimlerinin kısıtlanması önerilmektedir.

Sonuç olarak, bilgi ağlarıyla birbirine bağlanan bir dünyada, ortaya çıkan her yeni teknoloji bir taraftan fayda sağlarken diğer tarafta siber saldırıların ve güvenlik ihlallerinin hedefi haline gelmektedir. Kurumlar, siber saldırıların neden olduğu zararlara ilişkin çalışanlarının farkındalığını artırmalı ve bilgi ağlarını korumak için çalışanlarının siber hijyenini artıracak faaliyetleri benimsemek zorundadır.

Sınırlılıklar ve Gelecek Araştırmalara Öneriler

Her araştırmada olduğu gibi bu araştırmanın da kapsam, metodoloji, içerik ve örneklem konusunda bazı kısıtları bulunmaktadır. Öncelikle, ilk kısıt araştırmanın sektör olarak sadece BT çalışanlarına odaklanmış olmasıdır. BT çalışanlarına yapılan bu araştırmada, sektör noktasında kısıtlama yapılmıştır. Araştırmanın bir diğer kısıtı ise çalışma sonucunda elde edilen bulgular, örnekleme göre değişiklik gösterebileceğinden, mevcut çalışma sonunda yapılan değerlendirmeler verilerin toplandığı örneklem ile sınırlı olduğudur.

Bu çalışma kapsamında, algılanan güvenlik açığının, BT çalışanlarının siber hijyenini etkilemediği bulunmuştur. Algılanan güvenlik açığının bu çalışma kapsamında anlamsız çıkmasının nedeni çalışma örnekleminde yer alan BT çalışanlarının siber tehditlerin gerçekleşme ihtimali ve olası zararları hakkında bilinçli olmaları olabilir veya araştırma kısıtları ve sınırlılıkları nedeniyle bu çalışma dahilinde anlamlı çıkmamış olabilir. Bu nedenle gelecek araştırmalara bu konunun detaylı olarak ele alınması önerilmektedir.

Bu çalışma kapsamında anlamsız çıkan bir diğer faktör ise öznel normlardır. Öznel normların, BT çalışanlarının siber hijyenini etkilemediği bulunmuştur. Öznel normların bu çalışma kapsamında anlamsız çıkmasının nedeni, BT çalışanlarının, BT ve BT güvenliği yetenekleri konusunda, kendilerini tavsiyede bulunan diğer kişilerden daha bilgili düşündüklerinden ve kendilerine daha çok güvenmelerinden kaynaklı olabilir. Gelecek araştırmalara bu konunun detaylı olarak incelenmesi önerilmektedir.

Bu çalışma kapsamında, bilgi güvenliği politikalarına tutumun, BT çalışanlarının siber hijyenini etkilemediği bulunmuştur. Bunun nedeni, bilgi güvenliği politikalarının yetersiz olması veya güncel olmaması olabilir. BT çalışanlarının güvenlik konusunda diğer çalışanlardan daha bilgili olmaları olabilir veya kısıtları ve sınırlılıkları nedeniyle bu çalışma dahilinde anlamlı çıkmamış olabilir. Bu nedenle gelecek araştırmalara bu konunun detaylı olarak ele alınması önerilmektedir..

Bilgi güvenliği alanında araştırma yapmak ve veri toplamak kurumları tehlikeye atabileceğinden bu konuda kurumlardan bilgi almak oldukça zor olmaktadır. Ancak araştırma bulgularının genelleştirilmesi adına daha büyük bir örneklem büyüklüğü ve daha fazla sektör ile araştırma modelinin test edilmesi gelecek araştırmalara

önerilmektedir. Ayrıca örneklem grubuna farklı ülkelerin çalışanları katılarak ülkeler arası karşılaştırılma yapılması önerilmektedir. Sonuç olarak, organizasyonlarda siber güvenlik olaylarının nasıl önlenebileceği konusunda çalışanların siber hijyen davranışları ve siber güvenlik farkındalığı gibi insan faktörlerine odaklanılarak daha derinlemesine araştırmalar yapılması gerekmektedir.



KAYNAKÇA

- ABCNews. (2020). *NT Chief Minister delivers emotional address to Territorians about coronavirus shutdown* | ABC News - YouTube. <https://www.youtube.com/watch?v=QBV1gfcectU> adresinden 28.01.2021 tarihinde alınmıştır.
- Abdulhamid, S. M., Abd Latiff, M. S., Chiroma, H., Osho, O., Abdul-Salaam, G., Abubakar, A. I., ve Herawan, T. (2017). A review on mobile sms spam filtering techniques. *IEEE Access*, 5, 15650–15666. <https://doi.org/10.1109/ACCESS.2017.2666785>
- Aberdeen Group, W. S. (2015). *New research from aberdeen group and wombat security confirms security awareness and training measurably reduces cyber security risk*. <https://finance.yahoo.com/news/research-aberdeen-group-wombat-security-140000495.html> adresinden 12.04.2022 tarihinde alınmıştır.
- Abraham, S., ve Chengalur-Smith, I. S. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers ve Security*, 87, 101586. <https://doi.org/10.1016/J.COSE.2019.101586>
- Aigbefo, Q. A., Blount, Y., ve Marrone, M. (2022). The influence of hardiness and habit on security behaviour intention. *Behaviour and Information Technology*, 41(6), 1151–1170. <https://doi.org/10.1080/0144929X.2020.1856928>
- Ajzen, I. (1991). The theory of planned behavior. *Organization Behavior Human Decision Process*, 50, 179–211.
- Akbıyık, A. (2012). *Uzaktan eğitim ortamlarında sosyal yazılım kullanımının kabulünü etkileyen faktörleri belirlenmesine yönelik bir çalışma*. (Yayımlanmamış doktora tezi). Sakarya Üniversitesi
- Akdemir, N., ve Tuncer, C. O. (2021). *Siber ansiklopedi: siber ortama çok disiplinli bir yaklaşım*. Pegem Akademi Yayıncılık. Ankara
- Al-Emran, M., AlQudah, A. A., Abbasi, G. A., Al-Sharafi, M. A., ve Iranmanesh, M. (2023). Determinants of using ai-based chatbots for knowledge sharing: evidence from pls-sem and fuzzy sets (fsQCA). *IEEE Transactions on Engineering Management*, 99, 1–15. <https://doi.org/10.1109/tem.2023.3237789>
- Al-Shanfari, I., Yassin, W., Tabook, N., Ismail, R., ve Ismail, A. (2022). Determinants of information security awareness and behaviour strategies in public sector organizations among employees. *International Journal of Advanced Computer Science and Applications*, 13(8), 479–490. <https://doi.org/10.14569/IJACSA.2022.0130855>
- Alanazi, M., Freeman, M., ve Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, 121

136(December 2021), 107376. <https://doi.org/10.1016/j.chb.2022.107376>

- Albrechtsen, E., ve Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers and Security*, 28(6), 476–490. <https://doi.org/10.1016/j.cose.2009.01.003>
- AlGhanboosi, B., Ali, S., ve Tarhini, A. (2023). Examining the effect of regulatory factors on avoiding online blackmail threats on social media: A structural equation modeling approach. *Computers in Human Behavior*, 144(November 2022), 107702. <https://doi.org/10.1016/j.chb.2023.107702>
- Alkhalil, Z., Hewage, C., Nawaf, L., ve Khan, I. (2021). Phishing attacks: a recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3(March), 1–23. <https://doi.org/10.3389/fcoms.2021.563060>
- Allianz. (2020). *Allianz risk barometer 2020 - climate change | AGCS*. <https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2020-business-risks.html> adresinden 15.04.2021 tarihinde alınmıştır.
- Alraja, M. N., Butt, U. J., ve Abbod, M. (2023). Information security policies compliance in a global setting: An employee’s perspective. *Computers and Security*, 129, 103208. <https://doi.org/10.1016/j.cose.2023.103208>
- Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., ve Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, 73(August 2022), 102258. <https://doi.org/10.1016/j.techsoc.2023.102258>
- Ambalavanan, V., ve Shanthi Bala S. (2019). Cyber threats detection and mitigation using machine learning. M. Gupta (Ed.), *Advances in information security, privacy, and ethics* içinde (1.Baskı,132–149). IGI Global.
- APWG. (2016). *Phishing activity trends report* . <https://apwg.org/trendsreports/>
- APWG. (2021). *Phishing activity trends report* . <https://apwg.org/trendsreports/>
- Arachchilage, N. A. G., ve Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304–312. <https://doi.org/10.1016/j.chb.2014.05.046>
- Aronovich, A. (2018). *Why educating your employees on cyber intelligence and security will reduce risk*. <https://www.cybintsolutions.com/employee-education-reduces-risk/> adresinden 15.06.2022 tarihinde alınmıştır.
- Avcı, İ., Koca, M., ve Atasoy, M. (2021). Windows tabanlı uygulamalarda sql enjeksiyon siber saldırı senaryosu ve güvenlik önlemleri. *European Journal of Science and Technology*, 28, 213–219. <https://doi.org/10.31590/ejosat.995697>
- Awad, M., ve Foqaha, M. (2016). Email spam classification using hybrid approach of rbf neural network and particle swarm optimization. *International Journal of Network*

Security ve Its Applications, 8(5), 19–38.
<https://www.aaus.edu/publication/mohammed.awad/article/email-spam-classification-using-hybrid-approach-rbf-neural-network-and-particle-swarm-optimization>

- Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191–215.
- Barrett, S. (2007). Structural equation modelling: adjudging model fit. *Personality and individual differences*, 42, 815–824.
- Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems*, 1(2), 121–130. <https://doi.org/10.1057/ejis.1991.20>
- Batista, L., Silva, G., Araújo, V., Araújo, V., Rezende, T., Guimarães, A., ve Souza, S. (2018). Fuzzy neural networks to create an expert system for detecting attacks by SQL Injection. *The International Journal of Forensic Computer Science*, 13(1), 8–21. <https://doi.org/10.5769/j201801001>
- Bayuk, J. (2009). Enterprise Security for the Executive: Setting the Tone from the Tos. *Undefined*. Praeger. 978-0313376603
- Bayuk, J. L., Healey, J., Rohmeyer, S., Sachs, M. H., Schmidt, J., ve Weiss, J. (2012). *Cyber security policy guidebook*. Wiley; 1. Baskı. 978-1118027806
- Bélanger, F., Collignon, S., Enget, K., ve Negangard, E. (2017). Determinants of early conformance with information security policies. *Information and Management*, 54(7), 887–901. <https://doi.org/10.1016/j.im.2017.01.003>
- Biju, J. M., Gopal, N., ve Prakash, A. J. (2019). Cyber attacks and its different types. *International Research Journal of Engineering and Technology*, 6(3), 4849–4852. <https://www.irjet.net/archives/V6/i3/IRJET-V6I31244.pdf>
- Bindu, S. V., Mishra, R., ve Thilagam, S. S. (2018). Discovering spammer communities in twitter. *Journal of Intelligent Information Systems 2018* 51:3, 51(3), 503–527. <https://doi.org/10.1007/S10844-017-0494-Z>
- Blythe, J. M., ve Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, 87(August 2017), 87–97. <https://doi.org/10.1016/j.chb.2018.05.023>
- Bollen, K. A., ve Lennox, R. (1991). Conventional wisdom on measurement: a structural Equation Perspective. *Psychological Bulletin*, 110(2), 305–314.
- Boyd, S. W., ve Keromytis, A. D. (2004). SQLrand: preventing sql injection attacks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 3089, 292–302. https://doi.org/10.1007/978-3-540-24852-1_21

- Breda, F., Barbosa, H., ve Morais, T. (2017). Social engineering and cyber security. *INTED2017 Proceedings*, 1(August), 4204–4211. <https://doi.org/10.21125/inted.2017.1008>
- Brody, R. G., Mulig, E. V., ve Kimball, V. (2007). *Phishing, pharming and identity theft*. https://www.researchgate.net/publication/285678442_Phishing_pharming_and_identity_theft adresinden 12.02.2023 tarihinde alınmıştır.
- Bulgurcu, B., Cavusoglu, H., ve Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems*, 34(SPEC. ISSUE 3), 523–548. <https://doi.org/10.2307/25750690>
- Burns, A. J., Posey, C., Roberts, T. L., ve Benjamin Lowry, S. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, 68, 190–209. <https://doi.org/10.1016/j.chb.2016.11.018>
- Büyükılıç, M. (2018). *Cybersecurity framework for small and medium size enterprises*. (Yayımlanmamış yüksek lisans tezi) Bahçeşehir Üniversitesi.
- Büyüköztürk, Ş. (2005). *Sosyal bilimler için veri analizi el kitabı: istatistik, araştırma deseni, spss uygulamaları ve yorum*. (31. Baskı). Pegem Akademi Yayıncılık.
- Byrd, K., Her, E. S., Fan, A., Liu, Y., ve Leitch, S. (2022). Consumers' threat and coping appraisals of in-restaurant dining during a pandemic – The moderating roles of conflicting information and trust-in-science and scientists. *International Journal of Hospitality Management*, 103(January), 103186. <https://doi.org/10.1016/j.ijhm.2022.103186>
- Carlton, M., ve Levy, Y. (2017). Cybersecurity skills: foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management*, 5(2), 16–28. [https://doi.org/10.36965/ojakm.2017.5\(2\)16-28](https://doi.org/10.36965/ojakm.2017.5(2)16-28)
- Carver, C. S., ve Scheier, M. F. (1982). Control theory: a useful conceptual framework for personality-social, clinical, and health psychology. *Psychological Bulletin*, 92(1), 111–135.
- Chan, M., Woon, I., ve Kankanhalli, A. (2005). Perceptions of information security at the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, 1(3), 18–41.
- Check Point. (2023). *Average Weekly Global Cyberattacks peak with the highest number in 2 years, marking an 8% growth year over year, according to Check Point Research*. Check Point Research. <https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/> adresinden 02.02.2023 tarihinde alınmıştır.

- Chen, D. Q., ve Liang, H. (2019). Wishful thinking and it threat avoidance: an extension to the technology threat avoidance theory. *IEEE Transactions on Engineering Management*, 66(4), 552–567. <https://doi.org/10.1109/TEM.2018.2835461>
- Chen, H., ve Li, W. (2017). Mobile device users' privacy security assurance behavior A technology threat avoidance perspective. *Information and Computer Security*, 25(3), 330–344. <https://doi.org/10.1108/ICS-04-2016-0027>
- Chen, T. M., ve Robert, J. M. (2004). The evolution of viruses and worms. *Statistical Methods in Computer Security*, December 2004, 265–286. <https://doi.org/10.1201/9781420030884.ch16>
- Chen, Y., ve Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly: Management Information Systems*, 40(1), 205–222. <https://doi.org/10.25300/MISQ/2016/40.1.09>
- Cheng, L., Li, Y., Li, W., Holm, E., ve Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. *Computers and Security*, 39(PART B), 447–459. <https://doi.org/10.1016/j.cose.2013.09.009>
- Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, 295(2), 295–336.
- Chou, H. L., ve Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior*, 65, 334–345. <https://doi.org/10.1016/j.chb.2016.08.034>
- Cisco. (2014). *Data leakage worldwide: common risks and mistakes employees make*. www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html adresinden 12.02.2023 tarihinde alınmıştır.
- Claar, C. L., ve Johnson, J. J. (2012). Analyzing home pc security adoption behavior. *Journal of Computer Information Systems*, 52, 20-29.
- Clearswift. (2018). Cyber Security Incidents: Insider Threat falls in UK (to 65%) and Germany (to 75%) post GDPR, but US risk increases (to 80%) | Press Release. In *Clearswift Insider Threat Index 2018*. <https://www.clearswift.com/resources/press-releases/cybersecurity-incidents-insider-threat-falls-uk-and-germany-post-gdpr> adresinden 02.05.2023 tarihinde alınmıştır.
- Cobalt. (2024). *Top cybersecurity statistics*. <https://www.cobalt.io/blog/cybersecurity-statistics-2024> adresinden 02.05.2023 tarihinde alınmıştır.
- Cohen, F. (1987). Computer viruses. In *Computers and Security* (Vol. 6, Issue 1). <https://all.net/books/Dissertation.pdf>

- Conteh, N. Y., ve Schmick, S. J. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23), 31–38. <https://doi.org/10.19101/ijacr.2016.623006>
- Coşkun, C., Altunışık, R., Bayraktaroğlu, S., ve Yıldırım, E. (2015). *Sosyal bilimlerde araştırma yöntemleri- spss uygulamalı* (8. Baskı). Sakarya Kitabevi.
- Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, 28(5), 1849–1858. <https://doi.org/10.1016/j.chb.2012.05.003>
- Creswell-, J. W. (2014). *Research design qualitative, quantitative, and mixed methods approaches*. (4. Baskı). SAGE Publications, Inc
- Crossler, R., ve Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *Data Base for Advances in Information Systems*, 45(4), 51–71. <https://doi.org/10.1145/2691517.2691521>
- Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. <https://doi.org/10.1109/HICSS.2010.311>
- Crossler, R. E., Andoh-Baidoo, F. K., ve Menard, S. (2019). Espoused cultural values as antecedents of individuals’ threat and coping appraisal toward protective information technologies: Study of U.S. and Ghana. *Information and Management*, 56(5), 754–766. <https://doi.org/10.1016/j.im.2018.11.009>
- Crypsis. (2020). *Crypsis releases 2020 incident response and data breach report - cybersecurity magazine*. <https://cybersecurity-magazine.com/crypsis-releases-2020-incident-response-and-data-breach-report/> adresinden 03.06.2023 tarihinde alınmıştır.
- D’Arcy, J., ve Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20(6), 643–658. <https://doi.org/10.1057/ejis.2011.23>
- Dang-Pham, D., ve Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers and Security*, 48, 281–297. <https://doi.org/10.1016/j.cose.2014.11.002>
- Diamantopoulos, A., ve Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research*, 38(2), 269–277. <https://doi.org/10.1509/jmkr.38.2.269.18845>
- Diaz, A., Sherman, A. T., ve Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, 44(1), 53–67.

<https://doi.org/10.1080/01611194.2019.1623343>

- Dimopoulos, V., Furnell, S., Jennex, M., ve Kritharas, I. (2004). Approaches to it security in small and medium enterprises. In *AISM* (73–82). https://www.researchgate.net/publication/221148270_Approaches_to_IT_Security_in_Small_and_Medium_Enterprises
- Doane, A. N., Boothe, L. G., Pearson, M. R., ve Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computers in Human Behavior*, 60, 508–513. <https://doi.org/10.1016/J.CHB.2016.02.010>
- Dojkovski, S., Lichtenstein, S., ve Warren, M. (2006). Challenges in fostering an information security culture in australian small and medium sized enterprises. *5th European Conference on Information Warfare and Security 2006, ECIW 2006*, 31–40.
- Dojkovski, S., Lichtenstein, S., ve Warren, M. (2007). Fostering information security culture in small and medium size enterprises: an interpretive study in australia. *6th European Conference on Information Warfare and Security 2007, ECIW 2007*.
- Dojkovski, S., Lichtenstein, S., ve Warren, M. J. (2010). Enabling information security culture: Influences and challenges for Australian SMEs. *ACIS 2010 Proceedings - 21st Australasian Conference on Information Systems*.
- Douglas, D., Santanna, J. J., de Oliveira Schmidt, R., Granville, L. Z., ve Pras, A. (2017). Booters: can anything justify distributed denial-of-service (DDoS) attacks for hire? *Journal of Information, Communication and Ethics in Society*, 15(1), 90–104. <https://doi.org/10.1108/JICES-09-2016-0033>
- Douligeris, C., ve Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Computer Networks*, 44(5), 643–666. <https://doi.org/10.1016/j.comnet.2003.10.003>
- Edgar, T. W., ve Manz, D. O. (2017). Research methods for cyber security. In *Research Methods for Cyber Security*. [https://doi.org/10.1016/s1353-4858\(18\)30053-9](https://doi.org/10.1016/s1353-4858(18)30053-9)
- Ell, M., ve Gallucci, R. (2020). Cyber security breaches survey 2020. *Computer Fraud ve Security*, 2020(4), 4–4. [https://doi.org/10.1016/s1361-3723\(20\)30037-3](https://doi.org/10.1016/s1361-3723(20)30037-3)
- Emm, D. (2006). Phishing: phishing update, and how to avoid getting hooked. *Network Security*, 2006(8), 13–15
- Enisa. (2022). *Enisa a threat landscape report 2018 : 15 top cyber- threats and trends*. <https://os.europa.eu/en/publication-detail/-/publication/6373c334-574d-11e9-a8ed-01aa75ed71a1/language-en adresinden> 02.01.2022 tarihinde alınmıştır.
- Firdausi, I., Lim, C., Erwin, A., ve Nugroho, A. S. (2010). Analysis of machine learning techniques used in behavior-based malware detection. *Proceedings - 2010 2nd*

International Conference on Advances in Computing, Control and Telecommunication Technologies, ACT 2010, 201–203.
<https://doi.org/10.1109/ACT.2010.33>

Fischer, E. A., Ave, I., ve Washington, S. E. (2005). *CRS report for congress received through the crs web creating a national framework for cybersecurity : an analysis of.*

Floyd, D. L., Prentice-Dunn, S., ve Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429. <https://doi.org/10.1111/j.1559-1816.2000.tb02323.x>

Ene. C. (2023, 22 Şubat). *10.5 Trillion reasons why we need a united response to cyber risk*, Forbes. <https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/> adresinden 15.03.2024 tarihinde alınmıştır.

Fornell, C., ve Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 39–50.*

Forrester, V. V. (2019). *User information security behavior in professional virtual communities: a technology threat avoidance approach.* Nova Southeastern University.

Fowler, A., ve Everard, T. (2021). *What is cyber security culture and why does it matter for your organisation?*, <https://www.paconsulting.com/insights/what-is-cyber-security-culture-and-why-does-it-matter-for-your-organisation/> adresinden 12.11.2023 tarihinde alınmıştır.

Furnell, S., ve Clarke, N. (2005). Organizational security culture: Embedding security awareness, education, and training. *Proceedings of the 4th World Conference on Information Security Education, 11*(Dti), 67–74.

Furnell, S., ve Clarke, N. (2012). Power to the people? the evolving recognition of human aspects of security. *Computers and Security, 31*(8), 983–988. <https://doi.org/10.1016/j.cose.2012.08.004>

Furnell, S. M., Jusoh, A., ve Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers and Security, 25*(1), 27–35. <https://doi.org/10.1016/j.cose.2005.12.004>

Gaston, A., ve Prapavessis, H. (2014). Using a combined protection motivation theory and health action process approach intervention to promote exercise during pregnancy. *Journal of Behavioral Medicine, 37*(2), 173–184. <https://doi.org/10.1007/s10865-012-9477-2>

Geil, A., Sagers, G., Spaulding, A. D., ve Wolf, J. R. (2018). Cyber security on the farm: An assessment of cyber security practices in the United States agriculture industry.

International Food and Agribusiness Management Review, 21(3), 317–334.
<https://doi.org/10.22434/IFAMR2017.0045>

Gibbs, J. S. (1975). Crime, punishment, and deterrence. In *Elsevier*. Elsevier BV.

Gillam, A. R., ve Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior*, 108(June 2019), 106319. <https://doi.org/10.1016/j.chb.2020.106319>

Goodman, M. (2016). *Geleceğin suçları - dijital dünyanın karanlık yüzü*.(3.Baskı) Timaş Yayınları

Gorsuch, R. (1983). *Factor analysis* (2 Baskı). Psychology Press.

Greengard, S. (2016). *How spear phishing puts businesses on the hook*, Cioinsight. <https://www.cioinsight.com/security/how-spear-phishing-puts-businesses-on-the-hook/> adresinden 13.03.2023 tarihinde alınmıştır.

Grobler, M., Vuuren, J. C. J. van, ve Zaaïman, J. (2011). (PDF) *Evaluating cyber security awareness in South Africa*. https://www.researchgate.net/publication/228501727_Evaluating_cyber_security_awareness_in_South_Africa adresinden 13.03.2023 tarihinde alınmıştır.

Guilford, J. S. (1954). *Psychometric methods* (2 . Baskı). McGraw-Hill.

Guo, K. H., Yuan, Y., Archer, N., ve Connelly, C. (2011). Understanding nonmalicious security violations in the workplace: a composite behavior model. *Journal of Management Information Systems*, 28(1), 203–236.

Gürbüz, S. (2021). *AMOS ile Yapısal eşitlik modellemesi temel ilkeler ve uygulamalı analizler* (2. Baskı). Seçkin Yayıncılık.

Gürbüz, S., ve Şahin, F. (2018). *Sosyal bilimlerde araştırma yöntemleri*. (5. Baskı). Seçkin Yayıncılık.

Hair, J., Black, W., Babin, B., ve Anderson, R. (2014). Multivariate data analysis. In *International Journal of Multivariate Data Analysis* (7. Baskı). New Jersey:Pearson Prentice Hall.

Hair, J. F., Hult, G. T. M., Ringle, C. M., ve Sarstedt, M. (2016). A primer on partial least squares structural equation modeling (PLS-SEM). In *Sage* (2. Baskı). Sage.

Hair, J. F., Ringle, C. M., ve Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139–152. <https://doi.org/10.2753/MTP1069-6679190202>

Hair, J. F., Sarstedt, M., Hopkins, L., ve Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review*, 26(2), 106–121. <https://doi.org/10.1108/EBR-10->

- Halfond, W. G. J., Viegas, J., ve Orso, A. (2008). A Classification of sql injection attacks and countermeasures. *Preventing Sql Code Injection By Combining Static and Runtime Analysis*, 53.
- Hanus, B., Windsor, J. C., ve Wu, Y. (2018). Definition and multidimensionality of security awareness: Close encounters of the second order. *Data Base for Advances in Information Systems*, 49(s1), 103–132. <https://doi.org/10.1145/3210530.3210538>
- Hanus, B., ve Wu, Y. “Andy.” (2016). Impact of Users’ security awareness on desktop security behavior: a protection motivation theory perspective. *Information Systems Management*, 33(1), 2–16. <https://doi.org/10.1080/10580530.2015.1117842>
- Hatcher, L. (1994). *A step-by-step approach to using sas system for factor analysis and structural equation modeling*. SAS Institute.
- Henseler, J., Ringle, C. M., ve Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115–135. <https://doi.org/10.1007/s11747-014-0403-8>
- Herath, T., ve Rao, H. R. (2009a). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. <https://doi.org/10.1057/ejis.2009.6>
- Herath, T., ve Rao, H. R. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154–165. <https://doi.org/10.1016/j.dss.2009.02.005>
- Hoelter, J. W. (1983). The analysis of covariance structures: goodness-of-fit indices. *Sociological Methods ve Research*, 11, 325–344.
- Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, 55(1), 74–81. <https://doi.org/10.1145/2063176.2063197>
- Hooper, V., ve Blunt, C. (2019). Factors influencing the information security behaviour of IT employees. *Behaviour and Information Technology*, 39(8), 862–874. <https://doi.org/10.1080/0144929X.2019.1623322>
- Hoppe, F., Gatzert, N., ve Gruner, S. (2021). Cyber risk management in SMEs: insights from industry surveys. *Journal of Risk Finance*, 22(3–4), 240–260. <https://doi.org/10.1108/JRF-02-2020-0024>
- Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., ve Kalita, J. K. (2014). Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, 40(1), 307–324.

<https://doi.org/10.1016/j.jnca.2013.08.001>

- Hornetsecurity. (2022). *What is a computer worm? definition, difference to virus*. https://www.hornetsecurity.com/en/knowledge-base/computer-worm/?_adin=02021864894 adresinden 22.01.2023 tarihinde alınmıştır.
- Hosam, E., Hosny, H., Ashraf, W., ve Kaseb, A. S. (2021). SQL injection detection using machine learning techniques. *2021 8th International Conference on Soft Computing and Machine Intelligence, ISCMi 2021*, 15–20. <https://doi.org/10.1109/ISCMi53840.2021.9654820>
- Howarth, F. (2014). The role of human error in successful security attacks. *IBM Security Intelligence Website*, 1–6. <https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/>
- Humaidi, N., ve Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: the mediator effect of information security awareness. *International Journal of Information and Education Technology*, 5(4), 311–318. <https://doi.org/10.7763/ijiet.2015.v5.522>
- IBM. (2015). *Cyber security intelligence index*. <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WHveinfo&type=SAvehtml&fid=SEW03073USENveattachm&ent=SEW03073USEN.PDF> adresinden 22.01.2023 tarihinde alınmıştır.
- IBM. (2021). *Cost of a data breach hits record high during pandemic*. <https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic> adresinden 22.01.2023 tarihinde alınmıştır.
- IBM. (2023). *Cost of a data breach report*. <https://www.ibm.com/reports/data-breach>
- Ifinedo, S. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, 31(1), 83–95. <https://doi.org/10.1016/j.cose.2011.10.007>
- Ifinedo, S. (2014). Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, 51(1), 69–79. <https://doi.org/10.1016/j.im.2013.10.001>
- Jagatic, T. N., Johnson, N. A., Jakobsson, M., ve Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94–100. <https://doi.org/10.1145/1290958.1290968>
- Jarvis, C. B., Mackenzie, S. B., Podsakoff, S. M., Giliatt, N., ve Mee, J. F. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research*, 30(2), 199–218. <https://doi.org/10.1086/376806>

- Jindal, N., ve Liu, B. (2007). Review spam detection. *16th International World Wide Web Conference, WWW2007*, 1189–1190. <https://doi.org/10.1145/1242572.1242759>
- Johansen, A. G. (2020). *What is a trojan? Is It Virus or Malware? How It Works* | Norton. Norton - Security Centre. <https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html> adresinden 12.12.2022
- Johnson, J. C., Leeds, B. A., ve Wu, A. (2015). Capability, credibility, and extended general deterrence. *International Interactions*, 41(2), 309–336. <https://doi.org/10.1080/03050629.2015.982115>
- Johnston, A., ve Warkentin, M. (2010). Fear appeals and information security behaviors : an empirical study. *MIS Quarterly*, 34(3), 549–566.
- Johnston, A., Warkentin, M., ve Siponen, M. (2015). An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly* 39(1), 113–134.
- Joshi, M., Patil, B. V, ve Joshi, M. J. (2012). *A study of past, present computer virus ve perform-mance of selected security tools..* <https://www.researchgate.net/publication/288725457>
- Kaiser, H. F., ve Rice, J. (1974). Little jiffy, mark. IV. *Educational and Psychological Measurement*, 34(1), 111-117.
- Karayel, T., ve Akbıyık, A. (2023). Siber güvenlik araştırmalarına küresel bir bakış: yayın trendleri ve araştırma yönelimleri. *Bilişim Teknolojileri Dergisi*, 16(3), 221–235. <https://doi.org/10.17671/gazibtd.1291783>
- Kaspersky. (2019). What is Cyber Security? | Definition, types, and user protection | kaspersky. In *Www.Kaspersky.Co.Uk* (s. Home/Resource Centre/Definitions). <https://www.kaspersky.com.au/resource-center/definitions/what-is-cyber-security> adresinden 12.03.2023 tarihinde alınmıştır.
- Kaur Chahal, J., Bhandari, A., ve Behal, S. (2019). Distributed denial of service attacks: a threat or challenge. *New Review of Information Networking* (Vol. 24, Issue 1, 31–103). <https://doi.org/10.1080/13614576.2019.1611468>
- Khan, I. (2012). An introduction to computer viruses: Problems and solutions. *Library Hi Tech News*, 29(7), 8–12. <https://doi.org/10.1108/07419051211280036>
- Khan, N. F., Ikram, N., Murtaza, H., ve Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick’s Model. *Computers and Security*, 125. <https://doi.org/10.1016/j.cose.2022.103049>
- Kim, H. L., ve Han, J. (2019). Do employees in a “good” company comply better with information security policy? A corporate social responsibility perspective. *Information Technology and People*, 32(4), 858–875. <https://doi.org/10.1108/ITP-09-2017-0298>

- King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., ve Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in Psychology*, 9(FEB), 1–19. <https://doi.org/10.3389/fpsyg.2018.00039>
- Klimburg, A. (2012). *National cyber security framework manual*. <https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/>
- Kline, R. B. (2011). *Principles and practice of structural equation modeling*. (3. Baskı). Guilford Press.
- Knight, W. (2006). *Introduction: computer viruses*, Newscientist. <https://www.newscientist.com/article/dn9920-introduction-computer-viruses> adresinden 12.12.2022 tarihinde alınmıştır.
- Kramer, F. D., Starr, S. H., ve Wentz, L. K. (2009). *Cyberpower and national security*. (1. Baskı). Potomac books
- Kruger, H. A., ve Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, 25(4), 289–296. <https://doi.org/10.1016/j.cose.2006.02.008>
- Kuhalampi, M. (2017). *Impact of deterrence theory methods on employees' information security behavior*. Doktora Tezi.
- Kumar, A., Choi, B. J., Kuppusamy, K. S., ve Aghila, G. (2022). Malware attacks: dimensions, impact, and defenses. *Springer*. 157–179. https://doi.org/10.1007/978-3-030-90708-2_9
- Lazarus, R. S., ve Folkman, S. (1984). Stress, appraisal and coping. In *Springer*. Cambridge University Press.
- Lebek, B., Uffen, J., Neumann, M., Hohler, B., ve Breitner, M. H. (2014). Management research review information security awareness and behavior: a theory-based literature review) vequot;information security awareness and behavior: a theory-based literature reviewvequot; information security awareness and behavior: a theory-based. *Management Research Review*, 37(4), 1049–1092. <https://doi.org/10.1108/MRR-04-2013-0085>.
- Lee, Y., ve Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2), 177–187. <https://doi.org/10.1057/ejis.2009.11>
- Lehto, M., ve Neittaanmaki, S. (2015). Cyber security: analytics, technology and automation. In *intelligent systems, control and automation: science and engineering* (Vol. 78). <http://link.springer.com/10.1007/978-3-319-18302-2>
- Li, H., Zhang, J., ve Sarathy, R. (2010). Understanding compliance with internet use

- policy from the perspective of rational choice theory. *Decision Support Systems*, 48(4), 635–645. <https://doi.org/10.1016/J.DSS.2009.12.005>
- Li, L., He, W., Xu, L., Ash, I., Anwar, M., ve Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45(November 2018), 13–24. <https://doi.org/10.1016/j.ijinfomgt.2018.10.017>
- Li, L., Xu, L., ve He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, 5(December 2021). <https://doi.org/10.1016/j.chbr.2021.100165>
- Li, Y. J., ve Hoffman, E. (2023). Designing an incentive mechanism for information security policy compliance: An experiment. *Journal of Economic Behavior ve Organization*, 212, 138–159. <https://doi.org/10.1016/j.jebo.2023.05.033>
- Liang, H., ve Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly: Management Information Systems*, 33(1), 71–90. <https://doi.org/10.2307/20650279>
- Liang, H., ve Xue, Y. (2010a). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394–413. <https://doi.org/10.17705/1jais.00232>
- Liang, H., ve Xue, Y. (2010b). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394–413. <https://doi.org/10.17705/1jais.00232>
- Limayem, M., Hirt, S. G., ve Cheung, C. M. (2007). How habit limits the predictive power of intention: the case of information systems continuance. *MIS Q.*, 31(4), 705–737.
- Lowry, S. B., ve Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication*, 57(2), 123–146. <https://doi.org/10.1109/TPC.2014.2312452>
- Lu, Y., ve Xu, L. Da. (2019). Internet of things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, 6(2), 2103–2115. <https://doi.org/10.1109/JIOT.2018.2869847>
- Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing and Management*, 59(1), 102744. <https://doi.org/10.1016/j.ipm.2021.102744>
- MacKenzie, S. B., Podsakoff, S. M., ve Podsakoff, N. S. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly: Management Information Systems*, 35(2), 293–334. <https://doi.org/10.2307/23044045>

- Magdy, S., Abouelseoud, Y., ve Mikhail, M. (2022). Efficient spam and phishing emails filtering based on deep learning. *Computer Networks*, 206(January). <https://doi.org/10.1016/j.comnet.2022.108826>
- Mageshkumar, N., Vijayaraj, A., Arunpriya, N., ve Sangeetha, A. (2022). Efficient spam filtering through intelligent text modification detection using machine learning. *Materials Today: Proceedings*, xxxx. <https://doi.org/10.1016/j.matpr.2022.05.364>
- Mahn, A. (2018). *Identify, Protect, detect, respond and recover: the nist cybersecurity framework | nist*. National Institute of Standards and Technology. <https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework>
- Marett, K., McNab, A., ve Harris, R. (2011). Social networking websites and posting personal information: an evaluation of protection motivation theory. *AIS Transactions on Human-Computer Interaction*, 3(3). <https://aisel.aisnet.org/thci/vol3/iss3/2>
- Martínez Torres, J., Iglesias Comesaña, C., ve García-Nieto, S. J. (2019). Review: machine learning techniques applied to cybersecurity. In *International Journal of Machine Learning and Cybernetics* (Vol. 10, Issue 10, 2823–2836). <https://doi.org/10.1007/s13042-018-00906-1>
- Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, 50(4), 370–396. <https://doi.org/10.1037/H0054346>
- McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., ve Lillie, M. (2018). The effect of resilience and job stress on information security awareness. *Information and Computer Security*, 26(3), 277–289. <https://doi.org/10.1108/ICS-03-2018-0032>
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., ve Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151–156. <https://doi.org/10.1016/j.chb.2016.11.065>
- McMillan, R. (2021). *Beyond Colonial Pipeline, Ransomware Cyberattacks Are a Growing Threat - WSJ*. <https://www.wsj.com/articles/colonial-pipeline-hack-shows-ransomware-emergence-as-industrial-scale-threat-11620749675>
adresinden 12.12.2021 tarihinde alınmıştır.
- Medvet, E., Kirda, E., ve Kruegel, C. (2008). Visual-similarity-based phishing detection. *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, SecureComm'08*. <https://doi.org/10.1145/1460877.1460905>
- Menard, S., Bott, G. J., ve Crossler, R. E. (2017). User motivations in protecting information security: protection motivation theory versus self-determination theory. *Journal of management information systems*, 34(4), 1203–1230. <https://doi.org/10.1080/07421222.2017.1394083>

- Merkow, M. S., ve Breithaupt, J. (2014). *Information security principles and practices* (2. Baskı). Pearson IT Certification
- Mertler, C. A., ve Vannatta, R. A. (2005). *Advanced and multivariate statistical methods: Practical application and interpretation* (3. Baskı). Routledge.
- Microsoft. (2020). *Exploiting a crisis: How cybercriminals behaved during the outbreak* | Microsoft Security Blog. <https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/> adresinden 12.06.2023 tarihinde alınmıştır.
- Milne, S., Sheeran, S., ve Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 30(1), 106–143. <https://doi.org/10.1111/j.1559-1816.2000.tb02308.x>
- Mitropoulos, D., ve Spinellis, D. (2007). *Countering sql injection attacks with a database driver*. <https://www2.dmst.aueb.gr/dds/pubs/conf/2007-pcisqlia/html/ms07.htm> adresinden 03.03.2023 tarihinde alınmıştır.
- Mohammad, R. M., Thabtah, F., ve McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, 17, 1–24. <https://doi.org/10.1016/j.cosrev.2015.04.001>
- Mohammad, T., Mohamed Hussin, N. A., ve Husin, M. H. (2022). Online safety awareness and human factors: An application of the theory of human ecology. *Technology in Society*, 68(October 2021), 101823. <https://doi.org/10.1016/j.techsoc.2021.101823>
- Moody, G. D., Siponen, M., ve Pahlila, S. (2018). Toward a unified model of information security policy compliance. *MIS Q*, 42(1), 285–311. <https://doi.org/285-311>; DOI: 10.25300/MISQ/2018/13853
- Morgan, S. (2019). Global cybersecurity spending predicted to exceed \$1 trillion from 2017-2021. *Cybercrime Magazine*. <https://cybersecurityventures.com/cybersecurity-market-report/> adresinden 12.12.2022 tarihinde alınmıştır.
- Morgan, S. (2020). *Cybercrime To Cost The World \$10.5 Trillion Annually By 2025*. Cybersecurity Ventures. <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>
- Mou, J., Cohen, J. F., Bhattacharjee, A., ve Kim, J. (2022). A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach in Search Advertising. *Journal of the Association for Information Systems*, 23(1), 196–236.
- Mou, J., Cohen, J., ve Kim, J. (2018). A Meta-Analytic Structural Equation Modeling

Test of Protection Motivation Theory in Information Security Literature. *ICIS 2017: Transforming Society with Digital Innovation*. <http://aisel.aisnet.org/icis2017/Security/Presentations/5>

Nagin, D. S., ve Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology*, 39(4), 865–892. <https://doi.org/10.1111/J.1745-9125.2001.TB00943.X>

Nazneen, S., Xu, H., Ud Din, N., ve Karim, R. (2022). Perceived COVID-19 impacts and travel avoidance: application of protection motivation theory. *Tourism Review*, 77(2), 471–483. <https://doi.org/10.1108/TR-03-2021-0165>

NCS, B. (2022). *Siber saldırılar son zamanların zirvesinde!* <https://www.linkedin.com/pulse/siber-sald%25C4%25B1r%25C4%25B1lar-son-zamanlar%25C4%25B1n-zirvesinde-nsc-bili%25C5%259Fim-hizmetleri/?trackingId=5FaOVfbzqoVBzaC4SBDFAw%3D%3D> adresinden 12.12.2023 tarihinde alınmıştır.

Novikov, D. A. (2016). *Cybernetics : from past to future* (1. Baskı). Springer.

Nsugbe, E. (2021). A cybernetic framework for predicting preterm and enhancing care strategies: A review. framework for predicting preterm and enhancing care strategies: A review. *Biomedical Engineering Advances*, 2, 100024. <https://doi.org/10.1016/j.bea.2021.100024>

Orunsolu, A. A., Sodiya, A. S., ve Akinwale, A. T. (2022). A predictive model for phishing detection. *Journal of King Saud University - Computer and information sciences*, 34(2), 232–247. <https://doi.org/10.1016/J.JKSUCI.2019.12.005>

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers and Security*, 31(5), 673–680. <https://doi.org/10.1016/j.cose.2012.04.004>

Pahnila, S., Siponen, M., ve Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *Proceedings of the Annual hawaii international conference on system sciences, April*. <https://doi.org/10.1109/HICSS.2007.206>

Pandagle, V. (2023a). *Airbus cyber attack: work of usdod hacker, linked to turkish airlines employee account hack*. CyberExpress. <https://theycyberexpress.com/airbus-cyber-attack-usdod-turkish-airlines/> adresinden 14.04.2024 tarihinde alınmıştır.

Pandagle, V. (2023b). *Airbus cyber attack linked to turkish airlines account hack*, Thecyberexpress. <https://theycyberexpress.com/airbus-cyber-attack-usdod-turkish-airlines/> adresinden 14.04.2024 tarihinde alınmıştır.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., ve Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information

- Security Questionnaire (HAIS-Q). *Computers and Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
- Peace, A. G., Galletta, D. F., ve Thong, J. Y. L. (2003). Software piracy in the workplace: a model and empirical test. *Journal of Management Information Systems*, 20(1), 153–177. <https://doi.org/10.1080/07421222.2003.11045759>
- Pechmann, C., Zhao, G., Goldberg, M. E., ve Reibling, E. T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing*, 67(2), 1–18. <https://doi.org/10.1509/jmkg.67.2.1.18607>
- Petkauskas, V. (2024). *Attack on swedish datacenter shocks multiple businesses* | Cybernews. <https://cybernews.com/news/tietoevry-ransomware-attack-disrupts-businesses/>
- Pollock, T. (2017). *Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS)*. <http://digitalcommons.kennesaw.edu/ccerp%0Ahttp://digitalcommons.kennesaw.edu/ccerp/2017/research/2>
- Posey, C., Roberts, T. L., ve Lowry, S. B. (2015). The impact of organizational commitment on insiders motivation to protect organizational information assets. *Journal of Management Information Systems*, 32(4), 179–214. <https://doi.org/10.1080/07421222.2015.1138374>
- Posey, C., Roberts, T. L., ve Lowry, S. B. (2016). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Https://Doi.Org/10.1080/07421222.2015.1138374*, 32(4), 179–214. <https://doi.org/10.1080/07421222.2015.1138374>
- Proofpoint. (2020). *State of the phish report - stats, trends ve more*. <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish> adresinden 14.04.2024 tarihinde alınmıştır.
- Purkait, S. (2012). Phishing counter measures and their effectiveness - Literature review. *Information Management and Computer Security*, 20(5), 382–420. <https://doi.org/10.1108/09685221211286548>
- Pushpad, S., Juneja, C., ve Chawla, A. (2017). Triple phase protection technique to prevent sql injection attacks. *International journal of advance research in science and engineering*. 6(12) 1854–1863.
- Pwc. (2017). *UK organisations failing to prepare for cyber attacks*. <https://www.information-age.com/uk-organisations-still-failing-prepare-effectively-cyber-attacks-8270/>
- Qi, S. H., AlKulaib, L., ve Broniatowski, D. A. (2018). Detecting and characterizing bot-like behavior on twitter. *Lecture Notes in Computer Science (Including Subseries*

Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10899 LNCS, 228–232. https://doi.org/10.1007/978-3-319-93372-6_26

Quackenbush, S. L. (2011). Deterrence theory : where do we stand ? *Linked references are available on JSTOR for this article : Deterrence theory : where do we stand ?* 37(2), 741–762.

Rajab, M., ve Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers and Security*, 80, 211–223. <https://doi.org/10.1016/j.cose.2018.09.016>

Rao, S., Verma, A. K., ve Bhatia, T. (2021). A review on social spam detection: Challenges, open issues, and future directions. *Expert Systems with Applications*, 186(August), 115742. <https://doi.org/10.1016/j.eswa.2021.115742>

Reinartz, W., Haenlein, M., ve Henseler, J. (2009). An empirical comparison of the efficacy of covariance-based and variance-based SEM. *International Journal of Research in Marketing*, 26(4), 332–344. <https://doi.org/10.1016/j.ijresmar.2009.08.001>

Rhee, H. S., Kim, C., ve Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, 28(8), 816–826. <https://doi.org/10.1016/j.cose.2009.05.008>

Rogers, R. (1983). *Cognitive and physiological processes in fear appeals and attitude change: a revised theory of prote*. Guilford Press, New York, 153-177.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>

Rubin, A., ve Er, B. (2011). *Research methods for social work* (7. Baskı). Cengage Learning.

Saeed, S. (2023). A customer-centric view of e-commerce security and privacy. *Applied Sciences* , 13(2), 1020. <https://doi.org/10.3390/app13021020>

Safa, N. S., Solms, R. V., ve Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, 56, 70–82. <https://doi.org/10.1016/j.cose.2015.10.006>

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., ve Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, 53, 65–78. <https://doi.org/10.1016/j.cose.2015.05.012>

Salazar, L. F., Crosby, R. A., Noar, S. M., Walker, J. H., ve DiClemente, R. (2013). Models based on perceived threat and fear appeals. *Health Behavior Theory for Public Health*, 83–104.

- Samonas, S., ve Coss, D. (2014). The cia strikes back: redefining confidentiality, integrity and availability in security . *Journal of Information Security (JISec)*, 10(3), 21–45. www.jisec.org
- Sangani, N. K., ve Vijayakumar, B. (2012). Cyber security scenarios and control for small and medium enterprises. *Informatica Economica Journal*, 16(2), 58–71.
- Schatz, D., Bashroush, R., ve Wall, J. (2017). Towards a more representative definition of cyber security. *The Journal of Digital Forensics, Security and Law*, 12(2). <https://doi.org/10.15394/jdfsl.2017.1476>
- Schneier, B. (2004). *Secrets and lies digital security in a networked world* (15. Baskı). Wiley.
- Sekaran, U., ve Bougie, R. (2016). *Research methods for business: a skill building approach*. (7. Baskı). West Sussex: John Wiley ve Sons.
- Şenol, M. (2020). *Türkiye'nin ulusal siber güvenlik strateji ve politikalarının oluşturulması çerçevesinde caydırıcılık*. (Yayımlanmamış doktora tezi). İstanbul Teknik Üniversitesi.
- Sezgin, M. (2016). Bilişim devrimi, siberetik iletişim ve stratejik halkla ilişkiler. *Journal of Humanities and Tourism Research (Online)*, 6(6–2), 550–562. <https://doi.org/10.14230/joiss274>
- Shahbaznezhad, H., Kolini, F., ve Rashidirad, M. (2021). Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, 61(6), 539–550. <https://doi.org/10.1080/08874417.2020.1812134>
- Sharma, S., ve Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among IT employees. *Computers and Security*, 120. <https://doi.org/10.1016/j.cose.2022.102774>
- Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., ve Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE Access*, 8, 222310–222354. <https://doi.org/10.1109/ACCESS.2020.3041951>
- Shelly, G. B., ve Vermaat, M. E. (2012). *Discovering computers fundamentals*. http://mohduzir.uitm.edu.my/ECE431/Computers_Fundamentals.pdf adresinden 12.12.2022 tarihinde alınmıştır.
- Shmueli, G., ve Koppius, O. R. (2011). Predictive analytics in information systems research. *MIS Quarterly*, 35(3), 553–572.
- Shropshire, J., Warkentin, M., ve Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers and Security*, 49, 177–191. <https://doi.org/10.1016/j.cose.2015.01.002>

- Singleton, C., DeBeck, C., ve Chung, J. (2021). *Ibm security x-force threat intelligence index*, Ibm. <https://www.ibm.com/reports/threat-intelligence> adresinden 12.12.2021 tarihinde alınmıştır.
- Sinha, S., Rai, A. K., ve Bhushan, B. (2019). Information security threats and attacks with conceivable counteraction. *2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies Bildiriler kitabı içinde*, , (ss. 1208–1213). <https://doi.org/10.1109/ICICICT46008.2019.8993384>
- Siponen, M., Adam Mahmood, M., ve Pahnla, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, 51(2), 217–224. <https://doi.org/10.1016/j.im.2013.08.006>
- Siponen, M., Adam Mahmood, M., Pahnla, S., Shahbaznezhad, H., Kolini, F., Rashidirad, M., Khan, N. F., Ikram, N., Murtaza, H., Javed, M., ve Gibbs, J. S. (2021). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Information and Management*, 51(2), 217–224. <https://doi.org/10.1016/j.cose.2022.103049>
- Siponen, M., Pahnla, S., ve Mahmood, A. (2007). *Employees' Adherence to Information Security Policies: An Empirical Study*. Springer.
- Siponen, M. T. (2000). Conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, 8(1), 31–41. <https://doi.org/10.1108/09685220010371394>
- Soliman, W., ve Siponen, M. (2022). What do we really mean by rigor in information systems research? *Proceedings of the 55th Hawaii International Conference on System Sciences*. <https://doi.org/10.24251/hicss.2022.797>
- Solms, R., ve Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Sommestad, T., Karlzén, H., ve Hallberg, J. (2019). The theory of planned behavior and information security policy compliance. *Journal of Computer Information Systems*, 59(4), 344–353. <https://doi.org/10.1080/08874417.2017.1368421>
- Sonnemaker, T. (2021). *Google says gmail blocked 18 million coronavirus phishing emails*. <https://www.businessinsider.com/google-says-gmail-blocked-18-million-coronavirus-phishing-emails-2020-4> adresinden 05.05.2023 tarihinde alınmıştır.
- Spafford, E. H. (1994). Computer viruses as artificial life. *Artificial Life*, 1(3), 249–265. <https://doi.org/10.1162/artl.1994.1.3.249>
- Stanton, J. M., Stam, K. R., Mastrangelo, S., ve Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, 24(2), 124–133. <https://doi.org/10.1016/j.cose.2004.07.001>
- Stanton, J., Stam, K., Mastrangelo, S., ve Jolton, J. (2015). Behavioral information

security. *Human-Computer Interaction and Management Information Systems: Foundations*, 262–281.

Statista. (2024a). *Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023*. <https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/> adresinden 05.05.2024 tarihinde alınmıştır.

Statista. (2024b). *Fidye yazılımının hedefi olan küresel firmalar 2023* |. <https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/>

Stehr, N. (2007). Theories of the information age. In *The Handbook of Service Industries* (62–76). <https://doi.org/10.4337/9781847205261.00010> adresinden 05.05.2024 tarihinde alınmıştır.

Straub, D. W., ve Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly*, 14(1), 45. <https://doi.org/10.2307/249307>

Sulaiman, N. S., Fauzi, M. A., Hussain, S., ve Wider, W. (2022). cybersecurity behavior among government employees: the role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, 13(9). <https://doi.org/10.3390/info13090413>

Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., ve Harun, S. A. (2022b). Cyber-information security compliance and violation behaviour in organisations: a systematic review. *Social Sciences*, 11(9). <https://doi.org/10.3390/socsci11090386>

Sun, Y., Wang, N., ve Shen, X. L. (2020). Toward a configurational protection motivation theory. *Proceedings of the Annual Hawaii International Conference on System Sciences, 2020-Janua*, 3597–3606. <https://doi.org/10.24251/hicss.2020.440>

Symantec. (2020). *Executive summary 2019 internet security threat report*. <https://www.phishingbox.com/news/post/internet-security-threat-report-irst-2019> adresinden 12.12.2023 tarihinde alınmıştır.

Tabachnick, B. G., ve Fidell, L. S. (2007). Using multivariate statistics. In *Contemporary Psychology: A Journal of Reviews* (8 th, Vol. 28, Issue 8). Allyn ve Bacon/Pearson Education. <https://doi.org/10.1037/022267>

Tam, T., Rao, A., ve Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. In *Computers and Security* (Vol. 109, s. 102385). <https://doi.org/10.1016/j.cose.2021.102385>

Thompson, N., McGill, T. J., ve Wang, X. (2017). “Security begins at home”: Determinants of home computer and mobile device security behavior. *Computers and Security*, 70, 376–391. <https://doi.org/10.1016/j.cose.2017.07.003>

- Torten, R., Reaiche, C., ve Boyle, S. (2018). The impact of security awariness on information technology professionals' behavior. *Computers and Security*, 79, 68–79. <https://doi.org/10.1016/j.cose.2018.08.007>
- Trang, S., ve Brendel, B. (2019). A Meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers*, 21(6), 1265–1284. <https://doi.org/10.1007/S10796-019-09956-4/TABLES/8>
- Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., ve Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers and Security*, 59(1318885), 138–150. <https://doi.org/10.1016/j.cose.2016.02.009>
- Turner, W. (2016). *Cyber security for you* (1. Baskı). Independently published.
- Uchendu, B., Nurse, J. R. C., Bada, M., ve Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers and Security*, 109, 102387. <https://doi.org/10.1016/j.cose.2021.102387>
- Ulaştırma ve Altyapı Bakanlığı, U. (2020). *Kamuda stratejik yönetim | ulusal siber güvenlik stratejisi ve eylem planı (2020-2023)*. http://www.ss.gov.tr/tr/temel-belge/s/202/Ulusal+Siber+Guvenlik+Stratejisi+ve+Eylem+Plani+_2020-2023 adresinden 14.04.2023 tarihinde alınmıştır.
- Urbach, N., ve Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. *Journal of Information Technology Theory and Application (JITTA)*, 11(2), 5–40. <http://aisel.aisnet.org/jitta/vol11/iss2/2>
- Valli, C., Martinus, I., ve Johnstone, M. (2014). Small to medium enterprise cyber security awareness: an initial survey of western australian business. *Proceedings of the International Conference on Security and Management (SAM)*, 2020(July), 1.
- Vance, A., Siponen, M., ve Pahnla, S. (2012). Motivating is security compliance: insights from habit and protection motivation theory. *Information and Management*, 49(3–4), 190–198. <https://doi.org/10.1016/j.im.2012.04.002>
- Verizon. (2024). 2024 Data breach investigations report. *Verizon Business Journal*, 1–60. [file:///C:/Users/Edward S. Forde/Downloads/rp_Verizon-DBIR-2014_en_xg.pdf](file:///C:/Users/Edward%20S.%20Forde/Downloads/rp_Verizon-DBIR-2014_en_xg.pdf)
- Verkijika, S. F. (2019). “If you know what to do, will you take action to avoid mobile phishing attacks”: Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, 101(January), 286–296. <https://doi.org/10.1016/j.chb.2019.07.034>
- Verplanken, B., ve Orbell, S. (2003). Reflections on past behavior: a self-report index of habit strength. *Journal of Applied Social Psychology*, 33: 1313–1330.
- Von Solms, B., ve von Solms, R. (2018). Cybersecurity and information security – what

- goes where? *Information and Computer Security*, 26(1), 2–9. <https://doi.org/10.1108/ICS-04-2017-0025>
- Wall, J. D., ve Warkentin, M. (2019). Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics. *Information and Management*, 56(8), 103157. <https://doi.org/10.1016/j.im.2019.03.002>
- Wamala, F. (2011). Itü national cybersecurity strategy guide. *Chemistry September*, 122.
- Washo, A. H. (2021). Computers in human behavior reports an interdisciplinary view of social engineering : A call to action for research. *Computers in Human Behavior Reports*, 4, 100126. <https://doi.org/10.1016/j.chbr.2021.100126>
- Weinstein, N. D. (2000). Perceived probability, perceived severity, and health-protective behavior. *Health Psychology*, 19(1), 65–74. <https://doi.org/10.1037/0278-6133.19.1.65>
- Wen, H. J. (1998). Internet computer virus protection policy. *Information Management and Computer Security*, 6(2–3), 66–71. <https://doi.org/10.1108/09685229810209388>
- Wiener, N. (1948). *Cybernetics: control and communication in the animal and the machine*. Cambridge, MA: MIT Press.
- Williams, E. J., Hinds, J., ve Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120, 1–13. <https://doi.org/10.1016/J.IJHCS.2018.06.004>
- Williams, K. R., ve Hawkins, R. (1986). Perceptual research on general deterrence: a critical review. *Law ve Society Review*, 20(4), 545. <https://doi.org/10.2307/3053466>
- Willison, R., ve Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly: Management Information Systems*, 37(1), 1–20. <https://doi.org/10.25300/MISQ/2013/37.1.01>
- Woon, I., Tan, G.-W., ve Low, R. (2005). A Protection motivation theory approach to home wireless security. *International Conference on Information Systems (ICIS)*. <https://aisel.aisnet.org/icis2005/31>
- Workman, M., Bommer, W. H., ve Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799–2816. <https://doi.org/10.1016/j.chb.2008.04.005>
- Xin, T., Siponen, M., ve Chen, S. (2022). Understanding the inward emotion-focused coping strategies of individual users in response to mobile malware threats. *Behaviour ve Information Technology*, 41(13), 2835–2859.

<https://doi.org/10.1080/0144929X.2021.1954242>

- Yalçın, İ. (2019). *Soğuk savaş sonrası nato*. (Yayımlanmamış doktora tezi). Anadolu Üniversitesi.
- Yıldız, E. (2021). *SmartPLS ile yapısal eşitlik modellemesi reflektif ve formatif yapılar* (2. Baskı). Seçkin Yayıncılık.
- Yoon, C., Hwang, J.-W., ve Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, 23(4), 407–415.
- Young, D., Carpenter, D., ve Mcleod, A. (2016). Malware avoidance motivations and behaviors: a technology threat avoidance replication. *AIS Transactions on Replication Research*, 2(December), 1–17. <https://doi.org/10.17705/1attr.00015>
- Zargar, S. T., Joshi, J., ve Tipper, D. (2018). A Survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. *Computers and Electrical Engineering*, 72(4), 26–38. <https://doi.org/10.1016/j.compeleceng.2018.09.001>
- Zhang, J., Reithel, B. J., ve Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management and Computer Security*, 17(4), 330–340. <https://doi.org/10.1108/09685220910993980>
- Zhang, L., ve McDowell, W. C. (2009). Am i really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8(3–4), 180–197. <https://doi.org/10.1080/15332860903467508>

EKLER

Ek 1. Anket Formu

Değerli Katılımcı

Bu araştırma bireylerin bilgi ve bilgisayar güvenliği davranışını incelemek amacıyla yapılmaktadır. Bilgi ve bilgisayar güvenliği, siber saldırılara karşı kişisel, finansal ve sosyal bilgilerini korumak için bir dizi prosedüre uyma ve bazı güvenlik önlemlerini alma davranışlarının oluşturulmasını kapsamaktadır. Güvenlik ihlalleri, bilgisayar sistemine, önemli verilere ve uygulamalara yetkisiz erişim ile ulaşılması yoluyla oluşan olaylardır.

Anketten elde edilen verilerin bilimsel amaç dışında hiçbir kurum veya 3. şahıslar ile paylaşılmayacağını taahhüt eder katılımlarınız için çok teşekkür ederiz.

Doç. Dr. Adem AKBİYİK
Arş. Gör. Tuğçe KARAYEL
Sakarya Üniversitesi Yönetim Bilişim Sistemleri ABD Doktora Öğrencisi

Lütfen çalışmakta olduğunuz sektörü belirtiniz

☐ Bilişim	☐ Üretim	☐ Sağlık	☐ Hizmet
☐ Telekomünikasyon	☐ Bankacılık ve Finans	☐ Savunma	☐ Turizm
☐ Yapı	☐ Gıda	☐ Perakende	☐ Otomotiv

Şirketinizde ne şekilde çalışıyorsunuz belirtiniz.

☐ Uzaktan	☐ Hibrit (haftanın bazı günleri ofisten bazı günleri uzaktan)
----------------------------------	--

	1	2	3	4	5
	Kesinlikle Katılmıyorum	Katılmıyorum	Ne Katılıyorum	Katılıyorum	Kesinlikle Katılıyorum
Lütfen aşağıdaki soruları kurum işlerinizi yaptığınız bilgisayarı ve kurumunuzda kullandığınız bilgi sistemini düşünerek cevaplayınız.					
1- Güvenlik önlemlerine yeterince dikkat etmezsem çalıştığım kurumun bilgileri tehlikeye girebilir.	(1)	(2)	(3)	(4)	(5)
2- Çalıştığım kurumun bilgilerini koruma çabamın, bu bilgilere yasa dışı erişimi azaltacağını düşünüyorum.	(1)	(2)	(3)	(4)	(5)
3- Bilgi güvenliği politikasına uymazsam, çalıştığım kurumun güvenlik ihlallerine karşı savunmasız hale gelebileceğini düşünüyorum.	(1)	(2)	(3)	(4)	(5)
4- Bilgi güvenliği politikasına uymazsam, çalıştığım kurumun siber saldırıların hedefi haline gelebileceğini düşünüyorum.	(1)	(2)	(3)	(4)	(5)
1-Çalıştığım kurumun bilgilerini korumanın önemli olduğuna inanıyorum.	(1)	(2)	(3)	(4)	(5)
2-Şüpheli bir e-posta ekini açmam sonucunda bilgisayarıma virüs bulaşması benim için ciddi bir sorundur.	(1)	(2)	(3)	(4)	(5)
3-Çalıştığım kuruma yönelik gerçekleştirilen bilgi güvenliği ile ilgili siber saldırıları zarar verici görüyorum.	(1)	(2)	(3)	(4)	(5)

4-Bilgisayarımdaki bilgileri iznim olmadan birinin erişmesi benim için ciddi bir sorundur.	(1)	(2)	(3)	(4)	(5)
5-Bilgisayarıma siber saldırı düzenlenmesinden kaynaklanan veri kaybı benim için ciddi bir sorundur.	(1)	(2)	(3)	(4)	(5)
1- Güvenlik önlemlerini uygulamak çok zamanımı alıyor.	(1)	(2)	(3)	(4)	(5)
2- Güvenlik önlemlerini almak beni rahatsız ediyor.	(1)	(2)	(3)	(4)	(5)
3- Güvenlik önlemlerini uygulama ile elde edilen faydaların, güvenlik önlemlerinin maliyetini karşılamadığını düşünüyorum.	(1)	(2)	(3)	(4)	(5)
4- Güvenlik önlemlerini uygulamak iş yükümü artırıyor.	(1)	(2)	(3)	(4)	(5)
1-Güvenlik önlemlerini etkinleştirmek siber saldırıları önlemenin etkili bir yoludur.	(1)	(2)	(3)	(4)	(5)
2-Güvenlik önlemlerini uygulamak, kötü niyetli kişilerin kişisel veya finansal bilgileri erişmesini engelleyecektir.	(1)	(2)	(3)	(4)	(5)
3-Çalıştığım kurumun bilgilerini güvenlik ihlallerinden korumak için alınan mevcut önlemler yeterlidir.	(1)	(2)	(3)	(4)	(5)
4- Kötü niyetli kişilerin kurumun bilgi sistemine erişimini önlemek için kullanabileceğim önleyici tedbirler yeterlidir.	(1)	(2)	(3)	(4)	(5)
1-Kendimi bilgi güvenliği ihlallerinden korumak için gerekli becerilere sahibim.	(1)	(2)	(3)	(4)	(5)
2- Kötü niyetli kişilerin bilgileri erişmesini engellemek için önleyici tedbirler alacak uzmanlığa sahibim.	(1)	(2)	(3)	(4)	(5)
3- Kötü niyetli kişilerin bilgisayarıma erişimini engellemek için önleyici tedbirler alacak uzmanlığa sahibim.	(1)	(2)	(3)	(4)	(5)
4- Bilgi güvenliği ihlallerinden korunmanın kendi kontrolümde olduğuna inanıyorum.	(1)	(2)	(3)	(4)	(5)
5- Gerekli kılavuzlar olduğunda bilgisayarımda güvenlik önlemlerini aktif hale getirebilirim.	(1)	(2)	(3)	(4)	(5)
6- Bilgi güvenliği önlemlerini uygulamak benim için kolaydır.	(1)	(2)	(3)	(4)	(5)
1-Yöneticim güvenlik önlemlerini takip etmem gerektiğini düşünüyor.	(1)	(2)	(3)	(4)	(5)
2-Meslektaşlarım güvenlik önlemlerini takip etmem gerektiğini düşünüyor.	(1)	(2)	(3)	(4)	(5)
3-BT departmanı güvenlik önlemlerini takip etmem gerektiğini düşünüyor.	(1)	(2)	(3)	(4)	(5)
4-Astlarım güvenlik önlemlerini takip etmem gerektiğini düşünüyor.	(1)	(2)	(3)	(4)	(5)

1. Güvenlik önlemlerini uygulamak benim için bir alışkanlık haline gelmiştir.	(1)	(2)	(3)	(4)	(5)
2. Güvenlik önlemi almak düşünmeden yaptığım bir eylemdir.	(1)	(2)	(3)	(4)	(5)
3. Güvenlik önlemi almak rutininin bir parçasıdır.	(1)	(2)	(3)	(4)	(5)
1-Çalıştığım kurumun bilgi güvenliği politikasını takip etmek iyi bir fikirdir.	(1)	(2)	(3)	(4)	(5)
2- Çalıştığım kurumun bilgi güvenliği politikasını takip etmek bir zorunluluktur.	(1)	(2)	(3)	(4)	(5)
3- Çalıştığım kurumun bilgi güvenliği politikasını takip etmek faydalıdır.	(1)	(2)	(3)	(4)	(5)

	1	2	3	4	5
	Hiçbir Zaman	Nadiren	Ara Sıra	Sıklıkla	Her Zaman
Lütfen günlük bilgisayar kullanımında aşağıdaki siber hijyeni ilgilendiren maddelere ne sıklıkla dikkat ettiğinizi belirtiniz?					
1-Herhangi bir yeni USB bellek veya harici depolama cihazında virüs taraması yaparım	(1)	(2)	(3)	(4)	(5)
2-Bulut tabanlı bir sunucuda tüm önemli dosyaların yedeğini alırım (Google Drive, Dropox gibi)	(1)	(2)	(3)	(4)	(5)
3-Virüs koruma yazılımını güncel tutarım	(1)	(2)	(3)	(4)	(5)
4-Bir web sitesinin şifreleme kullanıp kullanmadığını görmek için web tarayıcısında kilit simgesini kontrol ederim (SSL olarak da bilinir)	(1)	(2)	(3)	(4)	(5)
5-Çevrimiçi finansal işlemler yaparken SSL sertifikasının kalitesini kontrol ederim	(1)	(2)	(3)	(4)	(5)
6-Halka açık internet ağlarında bilgisayarına diğer kişilerin elektronik ortamdaki erişimini yönetirim	(1)	(2)	(3)	(4)	(5)
7-Sosyal medya arkadaşlarının ve bilgi taleplerinin güvenilirliğini değerlendiririm	(1)	(2)	(3)	(4)	(5)
8-Sosyal medyada kimlerle arkadaş olduğumu bilirim	(1)	(2)	(3)	(4)	(5)
9-Sosyal medya arkadaşlarımı / bağlantılarımı yeniden değerlendiririm	(1)	(2)	(3)	(4)	(5)
10-Sosyal medya platformlarında gizlilik ayarlarımı yönetirim	(1)	(2)	(3)	(4)	(5)
11-İnternet erişimi olan tüm cihazlarda varsayılan şifreleri değiştiririm	(1)	(2)	(3)	(4)	(5)
12-Karmaşık kullanıcı adları ve şifreler oluştururum	(1)	(2)	(3)	(4)	(5)
13-Tüm çevrimiçi üyelikler için yeni / benzersiz kullanıcı adı ve şifreler oluştururum	(1)	(2)	(3)	(4)	(5)
14-Oturumlar için iki faktörlü veya çok faktörlü kimlik doğrulamayı etkinleştiririm (Sms veya e-mail ile kimlik ispatlama)	(1)	(2)	(3)	(4)	(5)
15-Gelen e-postanın başlığını kontrol ederim	(1)	(2)	(3)	(4)	(5)
16-E-posta gönderene kişinin, e-posta alan adını kontrol ederim (e-postalardaki @ işaretinden sonraki kısım)	(1)	(2)	(3)	(4)	(5)
17-E-postalardaki isteklerde dilbilgisi veya yazım hatası olup olmadığını kontrol ederim	(1)	(2)	(3)	(4)	(5)

Ek 2. Etik Kurul Onay Belgesi



T.C.
SAKARYA ÜNİVERSİTESİ REKTÖRLÜĞÜ
Etik Kurulu



Sayı : E-61923333-050.99-306484
Konu : 63/03 Tuğçe KARAYEL

17.11.2023

Sayın Tuğçe KARAYEL

İlgi : 10.11.2023 tarihli ve E--000-0 sayılı yazımız.

Üniversitemiz Sosyal ve Beşeri Bilimler Etik Kurulunun 15.11.2023 tarihli ve 63 sayılı toplantısında alınan "03" nolu karar ile Tuğçe KARAYEL'in başvurusu **uygun** görülmüş ve karar örneği ekte sunulmuştur.

Bilgilerinizi rica ederim.

Prof. Dr. Bayram TOPAL
Sosyal ve Beşeri Bilimler Etik Kurulu
Başkanı

Ek: Karar Yazısı (1 Sayfa)

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Doğrulama Kodu :BSLK9186T5 Pin Kodu :99242

Belge Takip Adresi : <https://turkiye.gov.tr/ebd?eK=5783&eD=BSLK9186T5&eS=306484>

Adres:Esentepe Kampüsü 54187 Serdivan SAKARYA / KEP Adresi:

sakaryauniversitesi@hs01.kep.tr

Telefon No:0264 295 50 00 Faks No:0264 295 50 31

e-Posta:ozelkalem@sakarya.edu.tr Elektronik Ağ:www.sakarya.edu.tr

Bilgi için: Hanife Babacan

Unvanı: Birim Evrak Sorumlusu



Ek 3. Smart PLS Analiz Sonuçları

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
AH1 -> CHBI	0.656	0.643	0.045	14.703	0.000
AH2 -> CHBI	0.715	0.701	0.047	15.243	0.000
AH3 -> CHBI	0.627	0.614	0.047	13.349	0.000
AH4 -> CHBI	0.700	0.687	0.056	12.591	0.000
EP1 -> CHBI	0.520	0.511	0.061	8.587	0.000
EP2 -> CHBI	0.533	0.522	0.058	9.148	0.000
EP3 -> CHBI	0.510	0.499	0.066	7.773	0.000
HBT1 <- HBT	0.944	0.944	0.005	174.311	0.000
HBT2 <- HBT	0.817	0.816	0.029	27.723	0.000
HBT3 <- HBT	0.921	0.921	0.008	117.339	0.000
ISP1 <- ISP	0.926	0.925	0.012	80.450	0.000
ISP2 <- ISP	0.808	0.808	0.025	32.607	0.000
ISP3 <- ISP	0.928	0.928	0.011	84.925	0.000
PS1 <- PS	0.740	0.739	0.042	17.656	0.000
PS2 <- PS	0.800	0.797	0.033	24.013	0.000
PS3 <- PS	0.726	0.723	0.047	15.520	0.000
PS4 <- PS	0.757	0.750	0.049	15.339	0.000
PS5 <- PS	0.800	0.796	0.035	22.608	0.000
PV1 <- PV	0.845	0.845	0.018	47.529	0.000
PV2 <- PV	0.822	0.822	0.025	32.877	0.000
PV3 <- PV	0.855	0.854	0.021	40.466	0.000
PV4 <- PV	0.829	0.827	0.024	35.052	0.000
RC1 <- RC	0.709	0.702	0.060	11.878	0.000
RC2 <- RC	0.849	0.848	0.023	37.219	0.000
RC3 <- RC	0.738	0.738	0.042	17.561	0.000
RC4 <- RC	0.754	0.748	0.049	15.507	0.000
RE1 <- RE	0.754	0.750	0.044	16.959	0.000
RE2 <- RE	0.788	0.784	0.038	20.739	0.000
RE3 <- RE	0.753	0.751	0.050	15.185	0.000
RE4 <- RE	0.769	0.766	0.050	15.344	0.000
SE1 <- SE	0.866	0.865	0.013	67.320	0.000
SE2 <- SE	0.903	0.903	0.010	93.305	0.000
SE3 <- SE	0.893	0.893	0.011	79.489	0.000
SE4 <- SE	0.661	0.661	0.033	20.159	0.000
SE5 <- SE	0.672	0.672	0.030	22.748	0.000
SE6 <- SE	0.833	0.833	0.020	41.344	0.000
SH1 -> CHBI	0.525	0.516	0.058	9.097	0.000
SH3 -> CHBI	0.664	0.652	0.050	13.358	0.000
SM1 -> CHBI	0.572	0.560	0.057	9.988	0.000
SM4 -> CHBI	0.536	0.525	0.055	9.703	0.000

SN1 <- SN	0.931	0.931	0.010	95.260	0.000
SN2 <- SN	0.930	0.930	0.010	97.144	0.000
SN3 <- SN	0.887	0.888	0.014	65.673	0.000
SN4 <- SN	0.908	0.908	0.013	72.411	0.000
TH1 -> CHBI	0.670	0.657	0.053	12.581	0.000
TH2 -> CHBI	0.703	0.689	0.047	14.932	0.000
TH3 -> CHBI	0.561	0.550	0.055	10.189	0.000

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
HBT	0.878	0.917	0.924	0.803
ISP	0.865	0.870	0.919	0.791
PS	0.825	0.834	0.876	0.586
PV	0.859	0.863	0.904	0.702
RC	0.783	0.828	0.848	0.584
RE	0.768	0.771	0.850	0.587
SE	0.892	0.907	0.919	0.658
SN	0.935	0.941	0.953	0.836

Fornell Larcker								
	HBT	ISP	PS	PV	RC	RE	SE	SN
HBT	0.896							
ISP	0.494	0.889						
PS	0.314	0.357	0.765					
PV	0.371	0.479	0.547	0.838				
RC	-0.372	-0.273	-0.186	-0.207	0.764			
RE	0.392	0.370	0.352	0.367	-0.298	0.766		
SE	0.678	0.391	0.304	0.401	-0.361	0.459	0.811	
SN	0.477	0.509	0.356	0.413	-0.203	0.311	0.351	0.914

HTMT								
	HBT	ISP	PS	PV	RC	RE	SE	SN
HBT								
ISP	0.555							
PS	0.360	0.414						
PV	0.408	0.554	0.635					
RC	0.415	0.278	0.189	0.196				
RE	0.473	0.452	0.424	0.435	0.359			
SE	0.757	0.450	0.351	0.454	0.396	0.560		

SN	0.512	0.567	0.401	0.460	0.200	0.364	0.383	
----	-------	-------	-------	-------	-------	-------	-------	--

	VIF		VIF
AH1	1.772	RC3	1.257
AH2	2.462	RC4	2.676
AH3	2.021	RE1	1.565
AH4	1.754	RE2	1.651
EP1	1.816	RE3	2.500
EP2	1.756	RE4	2.514
EP3	1.447	SE1	2.948
HBT1	3.841	SE2	4.794
HBT2	2.009	SE3	4.124
HBT3	2.972	SE4	1.513
ISP1	4.153	SE5	1.552
ISP2	1.592	SE6	2.357
ISP3	4.249	SH1	1.498
PS1	1.382	SH3	1.466
PS2	1.868	SM1	1.476
PS3	1.592	SM4	1.553
PS4	1.895	SN1	4.223
PS5	2.100	SN2	4.179
PV1	1.945	SN3	3.015
PV2	1.808	SN4	3.325
PV3	2.386	TH1	1.841
PV4	2.084	TH2	1.867
RC1	2.538	TH3	1.533
RC2	1.529		

Cross Loadings									
	CHBI	HBT	ISP	PS	PV	RC	RE	SE	SN
AH1	0.656	0.369	0.253	0.210	0.291	-0.279	0.184	0.373	0.307
AH2	0.715	0.481	0.285	0.205	0.285	-0.262	0.208	0.447	0.233
AH3	0.627	0.409	0.275	0.179	0.245	-0.161	0.195	0.397	0.245
AH4	0.700	0.469	0.299	0.149	0.272	-0.248	0.163	0.433	0.311
EP1	0.520	0.307	0.296	0.160	0.171	-0.235	0.164	0.285	0.179
EP2	0.533	0.354	0.196	0.190	0.169	-0.206	0.119	0.406	0.114
EP3	0.510	0.208	0.283	0.319	0.266	-0.164	0.142	0.283	0.127
HBT1	0.547	0.944	0.460	0.291	0.342	-0.366	0.349	0.633	0.430
HBT2	0.395	0.817	0.326	0.244	0.217	-0.287	0.316	0.528	0.313
HBT3	0.613	0.921	0.511	0.302	0.403	-0.340	0.383	0.648	0.507
ISP1	0.400	0.431	0.926	0.321	0.428	-0.274	0.339	0.337	0.434

ISP2	0.362	0.446	0.808	0.307	0.432	-0.190	0.284	0.344	0.476
ISP3	0.383	0.442	0.928	0.325	0.417	-0.259	0.362	0.362	0.449
PS1	0.354	0.280	0.335	0.740	0.519	-0.260	0.298	0.248	0.299
PS2	0.279	0.236	0.279	0.800	0.426	-0.126	0.236	0.240	0.269
PS3	0.229	0.186	0.230	0.726	0.392	-0.117	0.261	0.169	0.226
PS4	0.243	0.268	0.236	0.757	0.332	-0.093	0.290	0.261	0.243
PS5	0.282	0.214	0.258	0.800	0.380	-0.072	0.255	0.232	0.306
PV1	0.390	0.337	0.409	0.458	0.845	-0.186	0.246	0.335	0.368
PV2	0.367	0.342	0.419	0.460	0.822	-0.200	0.372	0.395	0.305
PV3	0.312	0.257	0.386	0.479	0.855	-0.155	0.287	0.301	0.347
PV4	0.337	0.295	0.385	0.437	0.829	-0.148	0.328	0.304	0.365
RC1	-0.131	-0.212	-0.091	-0.015	0.001	0.709	-0.176	-0.194	-0.056
RC2	-0.351	-0.342	-0.284	-0.189	-0.230	0.849	-0.208	-0.317	-0.190
RC3	-0.297	-0.297	-0.256	-0.220	-0.228	0.738	-0.305	-0.305	-0.232
RC4	-0.174	-0.228	-0.084	-0.023	-0.030	0.754	-0.197	-0.232	-0.044
RE1	0.230	0.308	0.323	0.351	0.380	-0.272	0.754	0.332	0.272
RE2	0.228	0.281	0.276	0.345	0.358	-0.255	0.788	0.350	0.253
RE3	0.170	0.289	0.292	0.185	0.171	-0.175	0.753	0.332	0.205
RE4	0.202	0.323	0.241	0.163	0.177	-0.195	0.769	0.394	0.210
SE1	0.528	0.572	0.305	0.206	0.325	-0.317	0.409	0.866	0.263
SE2	0.523	0.623	0.300	0.224	0.335	-0.267	0.385	0.903	0.309
SE3	0.525	0.614	0.321	0.250	0.364	-0.293	0.361	0.893	0.312
SE4	0.325	0.435	0.264	0.165	0.251	-0.144	0.369	0.661	0.206
SE5	0.449	0.432	0.372	0.320	0.315	-0.296	0.338	0.672	0.284
SE6	0.506	0.588	0.345	0.308	0.346	-0.400	0.384	0.833	0.321
SH1	0.525	0.319	0.232	0.223	0.214	-0.136	0.150	0.335	0.165
SH3	0.664	0.433	0.257	0.240	0.246	-0.234	0.200	0.384	0.268
SM1	0.572	0.269	0.277	0.253	0.287	-0.197	0.173	0.312	0.233
SM4	0.536	0.283	0.192	0.307	0.196	-0.246	0.134	0.339	0.149
SN1	0.365	0.459	0.489	0.319	0.386	-0.167	0.266	0.354	0.931
SN2	0.368	0.442	0.474	0.324	0.401	-0.171	0.269	0.302	0.930
SN3	0.298	0.426	0.452	0.355	0.356	-0.194	0.307	0.307	0.887
SN4	0.343	0.415	0.443	0.312	0.366	-0.215	0.299	0.321	0.908
TH1	0.670	0.379	0.288	0.284	0.310	-0.227	0.143	0.419	0.218
TH2	0.703	0.419	0.277	0.295	0.299	-0.219	0.166	0.452	0.243
TH3	0.561	0.359	0.188	0.237	0.243	-0.181	0.139	0.321	0.238

	Difference (Uzaktan- Hibrit)	1-tailed (Uzaktan vs Hibrit) p value	2-tailed (Uzaktan vs Hibrit) p value
HBT -> CHBI_GENEL	0.296	0.009	0.009

ISP -> CHBI_GENEL	-0.145	0.890	0.110
PS -> CHBI_GENEL	-0.023	0.584	0.416
PV -> CHBI_GENEL	-0.096	0.796	0.204
RC -> CHBI_GENEL	0.018	0.407	0.407
RE -> CHBI_GENEL	0.057	0.259	0.259
SE -> CHBI_GENEL	-0.157	0.910	0.090
SN -> CHBI_GENEL	0.022	0.428	0.428



ÖZGEÇMİŞ

Adı Soyadı: Tuğçe KARAYEL

ÖĞRENİM DURUMU

Öğrenim Derecesi	Öğrenim Yeri	Öğrenim Yılı
Doktora	Sakarya Üniversitesi /İşletme Enstitüsü / Yönetim Bilişim Sistemleri	2024
Yüksek Lisans	Sakarya Üniversitesi /İşletme Enstitüsü / Yönetim Bilişim Sistemleri	2019
Lisans	Bartın Üniversitesi / İktisadi ve İdari Bilimler Fakültesi / Yönetim Bilişim Sistemleri	2016
Lise	Melek Aknıl Anadolu Teknik Lisesi	2012

İŞ DENEYİMİ

Yıl	Yer	Görev
2019- Devam	Düzce Üniversitesi	Araştırma Görevlisi

YABANCI DİL

İngilizce

ESERLER

Karayel, T., Aktaş, B., ve Akbıyık, A. (2024). Human factors in remote work: examining cyber hygiene practices. *Information ve Computer Security*. DOI 10.1108/ICS-11-2023-0215

Karayel, T. ve Akbıyık, A. (2023). Siber güvenlik araştırmalarına küresel bir bakış: yayın trendleri ve araştırma yönelimleri. *Bilişim Teknolojileri Dergisi* 16(3) 221-235

Koç, T., Karayel, T., Demir, E. ve Akbıyık, A. (2023) *A systematic review of the research on cyberchondria*. 10th International Management Information Systems Conference [sözlü sunum]. İstanbul, Türkiye.

- Karayel, T. ve Kurutkan, M. N. (2022). Covid-19 sürecinde yapay zekâ ve bileşenleri ile ilgili yayınların bibliyometrik analizi. *Sağlık Akademisyenleri Dergisi*,9(3): 220-233 Doi: 10.52880/Sagakaderg.1070774
- Aslan, T., Aktaş, B., ve Akbıyık, A. (2020). *Kullanıcıların bilgisayar güvenliği davranışını inceleme: siber hijyen*. 7. Uluslararası Yönetim Bilişim Sistemleri Konferansı [sözlü sunum]. İstanbul, Türkiye.
- Aslan, T. ve Akbıyık, A. (2020) Empowering the economic impact of virtual communities: managing trust in the sharing economy S. Alavi, V Ahuja (Ed.) *Managing social media practices in the digital economy* (1. Baskı, ss 312) ISBN:9781799821854,
- Aslan, T. ve Akbıyık, A. (2020) The impact of circular economy on the fashion industry: a research on clothing share services A. Shrivastava, G. Jain, J. Paul (Ed.) *Circular economy and re-commerce in the fashion industry*, (1. Baskı, ss 204) ISBN:9781799827290,
- Aslan, T., Polat, M., ve Akbıyık, A. (2019). *Paylaşım ekonomisi müşteri memnuniyetini etkiliyor mu? konaklama hizmetlerine yönelik karşılaştırmalı bir analiz*. 6. Uluslararası Yönetim Bilişim Sistemleri Konferansı [sözlü sunum]. İstanbul, Türkiye.
- Aslan, T. ve Akbıyık A. (2019). Paylaşım ekonomisinde mülk paylaşma hizmetlerine duyulan güven rolünü tüketici perspektifinden inceleme: airbnb örneği. *İşletme Araştırmaları Dergisi*, 11(3), 2322-2332., Doi: <https://doi.org/10.20491/Isarder.2019.742>
- Aslan, T. ve Akbıyık, A. (2018) Mobil trafik uygulamaları üzerine tüketici yorumlarının içerik analizi: ibb cep trafik uygulama örneği, S.Gülseçen (Ed.) *Yönetim bilisim sistemlerinde gündem içinde* (1.Baskı, ss 10) Çağlayan Yayınevi, ISBN:9789754361537
- Aslan, T., Çakar, E., ve Akbıyık, A. (2017). *Türkiye’de yönetim bilişim sistemleri alanındaki araştırmaların bilimetrik bir analizi*. 4. Uluslararası Yönetim Bilişim Sistemleri Konferansı [Özet Bildiri/Poster]. İstanbul, Türkiye.
- Aslan, T. ve Akbıyık, A. (2017). *Mobil trafik uygulamaları üzerine tüketici yorumlarının içerik analizi: ibb cep trafik uygulama örneği*. 4. Uluslararası Yönetim Bilişim Sistemleri Konferansı [sözlü sunum]. İstanbul, Türkiye.