T.C.
FIRAT ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ

KURUMSAL BİLGİ GÜVENLİĞİNİN ÖRGÜTSEL İLETİŞİM, ÖRGÜTSEL BİLGİ PAYLAŞIMI VE KİŞİSEL BİLGİ GÜVENLİĞİ FARKINDALIĞI AÇISINDAN DEĞERLENDİRİLMESİ

Ebru POLAT

Doktora Tezi

TEKNOLOJİ VE BİLGİ YÖNETİMİ ANABİLİM DALI

EKİM 2022

T.C.
FIRAT ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ

TEKNOLOJİ VE BİLGİ YÖNETİMİ ANA BİLİM DALI

Doktora Tezi

KURUMSAL BİLGİ GÜVENLİĞİNİN ÖRGÜTSEL İLETİŞİM, ÖRGÜTSEL BİLGİ PAYLAŞIMI VE KİŞİSEL BİLGİ GÜVENLİĞİ FARKINDALIĞI AÇISINDAN DEĞERLENDİRİLMESİ

Tez Yazarı
Ebru POLAT

Danışman
Prof. Dr. Ahmet TEKİN

EKİM 2022
ELAZIĞ

T.C.

FIRAT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

TEKNOLOJİ VE BİLGİ YÖNETİMİ ANA BİLİM DALI

Doktora Tezi

Başlığı:	KURUMSAL BİLGİ GÜVENLİĞİNİN ÖRGÜTSEL İLETİŞİM, ÖRGÜTSEL BİLGİ PAYLAŞIMI VE KİŞİSEL BİLGİ GÜVENLİĞİ FARKINDALIĞI AÇISINDAN DEĞERLENDİRİLMESİ
Yazarı:	Ebru POLAT
Tez Öneri Tarihi:	13.12.2019
Savunma Tarihi:	19.10.2022

TEZ ONAYI

Fırat Üniversitesi Sosyal Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda **OYBİRLİĞİ/~~OYÇOKLUĞU~~** ile kabul edilmiştir**.**

İmza

Danışman:	**Prof. Dr. Ahmet TEKİN** Fırat Üniversitesi Eğitim Fakültesi
Başkan:	**Prof. Dr. Engin KURŞUN** Atatürk Üniversitesi Kâzım Karabekir Eğitim Fakültesi
Üye:	**Doç. Dr. Cem AYDEN** Fırat Üniversitesi İktisadi ve İdari Bilimler Fakültesi
Üye:	**Doç. Dr. Muhammed ZİNCİRLİ** Fırat Üniversitesi Eğitim Fakültesi
Üye:	**Dr.Öğr. Üyesi Seda İŞGÜZAR** Turgut Özal Üniversitesi İşletme ve Yönetim Bilimleri Fakültesi

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.
Prof. Dr. Murat SUNKAR
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Sosyal Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım **"KURUMSAL BİLGİ GÜVENLİĞİNİN ÖRGÜTSEL İLETİŞİM, ÖRGÜTSEL BİLGİ PAYLAŞIMI VE KİŞİSEL BİLGİ GÜVENLİĞİ FARKINDALIĞI AÇISINDAN DEĞERLENDİRİLMESİ"** Başlıklı Doktora Tezi'min içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

Ekim 2022

Ebru POLAT

ÖN SÖZ

Bilgi varlıklarında yaşanan artış, güvenlik ihlalleri nedeni ile meydana gelen hasarlar kurumların bilgi güvenliği için önlemler almalarını zorunlu kılmaktadır. Kurumlar bilgi varlıklarını korumak için teknolojik önlemler almaktadır. Ancak kurumsal bilgi güvenliğinin sağlanmasında teknik önlemlerin yanı sıra insan ve örgüt faktörünün de dikkate alınması gerekmektedir. Üniversiteler birçok bilgi kaynağını bir arada bulundurması sebebiyle bilgi güvenliği tehditleri ile karşı karşıya kalmaktadır. Bu nedenle, gerçekleştirilen tez çalışmasında üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği; kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı bağlamında incelenmiştir. Araştırma sonucunda alan yazında yer alan teorik bilgilere nicel kanıtlar sunulması hedeflenmiştir. Ayrıca kurumsal bilgi güvenliği ile kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı arasındaki ilişkiye yönelik elde edilen bulgularla alan yazına katkı sağlayacağı düşünülmektedir.

Lisansüstü eğitime başladığım ilk günden bugüne bilgi ve tecrübelerinden faydalandığım, her zaman güvenini, desteğini ve yardımını benden esirgemeyen; akademik bakış açısını ve çalışma disiplinini örnek aldığım, üzerimde büyük emeği olan kıymetli danışman hocam Prof. Dr. Ahmet TEKİN'e teşekkürlerimi sunarım.

Tez çalışmama olan katkılarından ve önerilerinden dolayı kıymetli hocalarım Doç. Dr. Cem AYDEN'e ve Doç. Dr. Muhammed ZİNCİRLİ'ye teşekkürlerimi sunarım.

Her türlü konuda içtenlikle yardımlarını esirgemeyen, bilgi ve tecrübelerinden faydalandığım kıymetli hocalarım Doç. Dr. Oğuzhan ÖZDEMİR'e, Doç. Dr. Songül KARABATAK'a, Doç. Dr. Tuncay Yavuz ÖZDEMİR'e ve Prof. Dr. Yalın Kılıç TÜREL'e teşekkürlerimi sunarım.

Destekleri ile yanımda olan, kıymetli dostlarım Elçin AYAZ'a ve Zeynep ÖZTEKİN'e verdiği manevi destekten dolayı teşekkür ederim. Ayrıca destekleri ile yanımda olan iş arkadaşlarıma teşekkür ederim.

Hayatım boyunca bana her zaman her anlamda destek olan, inanan, sevgi ve sabırlarıyla güç veren, fedakârlık gösteren sevgili aileme en içten sevgi ve teşekkürlerimi sunarım.

Ebru POLAT

ELAZIĞ 2022

İÇİNDEKİLER

ÖZET

KURUMSAL BİLGİ GÜVENLİĞİNİN ÖRGÜTSEL İLETİŞİM, ÖRGÜTSEL BİLGİ PAYLAŞIMI VE KİŞİSEL BİLGİ GÜVENLİĞİ FARKINDALIĞI AÇISINDAN DEĞERLENDİRİLMESİ

Ebru POLAT

Doktora Tezi

FIRAT ÜNİVERSİTESİ

Sosyal Bilimleri Enstitüsü

TEKNOLOJİ VE BİLGİ YÖNETİMİ ANA BİLİM DALI

Ekim 2022, Sayfa: XIII + 122

Teknolojide yaşanan gelişmeler, bilgi varlıklarında yaşanan artış kurumsal bilgi güvenliğinin giderek önem kazanmasına neden olmaktadır. İlgili alan yazın incelendiğinde kurumsal bilgi güvenliğinin sağlanmasında yalnızca teknik önlemlerin alınmasının yeterli olmadığı görülmüştür. Kurumsal bilgi güvenliğinin sağlanmasında örgütsel ve bireysel özellikler de dikkate alınmalıdır. Bu bağlamda tez çalışmasının amacı, üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliğinin, örgütsel iletişim, örgütsel bilgi paylaşımı ve kişisel bilgi güvenliği farkındalığı açısından değerlendirilmesidir. Araştırmada nicel araştırma yöntemlerinden ilişkisel tarama modeli benimsenmiştir. Ayrıca veri madenciliğinin tahmin edici modelleri kullanılmıştır. Tez çalışmasında Kurumsal Bilgi Güvenliği (Gerçeker, 2012), Bilgi Güvenliği Farkındalık Düzeyi Belirleme (Keser ve Güldüren, 2015), Örgütsel Bilgi Paylaşım (Aslan, 2014) ölçekleri ve standardizasyon işlemleri araştırmacı tarafından gerçekleştirilen Örgütsel İletişim Envanteri (Tuna, 2008) kullanılmıştır. Çalışmanın evrenini Türkiye'nin doğusunda yer alan bir üniversitede görev yapan akademik ve idari personel oluşturmaktadır. Türkiye'nin doğusunda yer alan bir üniversitede görev yapan 479 akademik ve idari personelden alınan veriler üzerinden analizler gerçekleştirilmiştir. Elde edilen verilerle doğrulayıcı faktör analizi, korelasyon, regresyon ve yapısal eşitlik modeli analizleri gerçekleştirilmiştir. Aynı zamanda veri madenciliğinin tahmin edici modellerinden, Destek Vektör Makineleri, Yapay Sinir Ağları, K-En Yakın Komşu ve Rastgele Orman algoritmaları kullanılmıştır. Verilerin normal dağılımını belirlemek için basıklık ve çarpıklık değerleri hesaplanmış, normal dağılımın olması nedeni ile Bağımsız Gruplar t-Testi ve Anova testi gerçekleştirilmiştir. Gerçekleştirilen Bağımsız Gruplar t-Testi ve Anova testi sonucunda anlamlı farklılığın etki büyüklüğünü belirlemek amacı ile eta-kare ($\eta 2$) ve Cohen d değerleri hesaplanmıştır.

Araştırma sonucunda, üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği, bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşım düzeyinin yüksek olduğu belirlenmiştir. Demografik bilgilere göre yapılan farklılık analizi sonucunda, kurumsal bilgi güvenliğinin İnternette/ sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenlerine göre anlamlı farklılık gösterdiği; bilgi güvenliği farkındalığının yaş, hizmet süresi, İnternette/ sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenlerine göre anlamlı farklılık gösterdiği; örgütsel bilgi paylaşımının ise yaş, hizmet süresi, İnternette/ sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenlerine göre anlamlı farklılık gösterdiği belirlenmiştir.

Gerçekleştirilen regresyon analizi sonucunda kişisel bilgi güvenliği farkındalığının, örgütsel iletişimin ve örgütsel bilgi paylaşımının kurumsal bilgi güvenliğini anlamlı şekilde yordadığı sonucuna ulaşılmıştır. Araştırma değişkenlerinin kurumsal bilgi güvenliği ile ilişkisini belirlemek amacıyla gerçekleştirilen yol

analizi sonuçları da regresyon analizi sonucuna benzerlik göstermektedir. Bu sonuçlara göre üniversitelerde bilgi güvenliği farkındalığı düzeyinin ve örgütsel iletişimin yüksek olması kurumsal bilgi güvenliğini olumlu yönde etkilemektedir. Ayrıca örgütsel iletişim, örgütsel bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi bulunduğu sonucuna ulaşılmıştır. Üniversitelerde görev yapan akademik ve idari personelin kişisel bilgi güvenliği farkındalığını arttırmaya yönelik yapılacak planlamaların, kurumsal bilgi güvenliğine olumlu katkı sağlayacağı düşünülmektedir. Aynı zamanda kurum içerisindeki formel iletişimin teşvik edilerek kurumsal bilgi güvenliğinin sağlanmasını olumlu etkileyeceği söylenebilir. Kurum içerisindeki formel iletişimin arttırılarak örgütsel bilgi paylaşımının teşvik edilmesi; böylelikle kurumsal bilgi güvenliğinin sağlanmasına olumlu katkıda bulunacağı düşünülmektedir.

Anahtar Kelimeler: Bilgi güvenliği, kurumsal bilgi güvenliği, örgütsel iletişim, örgütsel bilgi paylaşımı.

ABSTRACT

Evaluation of Corporate Information Security in terms of Organizational Communication, Organizational Knowledge Sharing and Personal Information Security Awareness

Ebru POLAT

Ph.D. Thesis

FIRAT UNIVERSITY

Graduate School of Social Sciences

Technology and Knowledge Management

October 2022, Page: XIII + 122

The developments in technology and the increase in information assets cause corporate information security to become increasingly important. The relevant literature revealed that taking only technical measures is not sufficient to ensure corporate information security. Organizational and individual characteristics should also be taken into account in ensuring corporate information security. In this context, the aim of the study is to evaluate the institutional information security of the academic and administrative staff working at a university in the context of organizational communication, organizational knowledge sharing, and personal information security awareness. Correlational survey model, which is one of the quantitative research methods, was adopted in the study. In addition, predictive models of data mining were used. The population of the study consists of academic and administrative staff working in a university located in the east of Turkey. The participants consist of 479 academic and administrative personnel. In the study, Corporate Information Security Scale (Gerçeker, 2012), Information Security Awareness Level Determination Scale (Keser and Güldüren, 2015), Organizational Knowledge Sharing Scale (Aslan, 2014) and the Organizational Communication Inventory (Tuna, 2008), whose standardization processes were carried out by the researcher, were used. Confirmatory factor analysis, correlation, regression, and structural equation model analyzes were performed with the obtained data. In addition, the predictive models of data mining, Support Vector Machines, Artificial Neural Networks, K-Nearest Neighbor, and Random Forest algorithms were used. In order to determine the normal distribution of the data, the kurtosis and skewness values were calculated. Since the data were normally distributed, an independent samples t-test and ANOVA test were performed. Eta-square (η2) and Cohen d values were calculated in order to determine the effect size of the significant difference as a result of the independent samples t-test and ANOVA test.

As a result of the study, it was determined that the academic and administrative staff working at the university had a high level of institutional information security, information security awareness, organizational communication, and organizational knowledge sharing. As a result of the difference analysis conducted according to demographic information, it was found that corporate information security differs significantly according to the frequency of checking privacy/security settings on the Internet/social networking sites; information security awareness differs significantly according to age, duration of service, frequency of checking privacy/security settings on the Internet/social networking sites; organizational knowledge sharing differs significantly according to age, length of service, and frequency of checking privacy/security settings on the Internet/social networking sites.

As a result of the regression analysis, it was concluded that personal information security awareness, organizational communication, and organizational knowledge sharing significantly predicted corporate information security. The results of the path analysis carried out to determine the relationship between the variables and corporate information security were also similar to the results of the regression analysis.

According to these results, a high level of information security awareness and organizational communication in universities positively affected corporate information security. In addition, it was concluded that organizational communication and organizational knowledge sharing had a mediating effect on corporate information security. It is expected that making plans to increase the awareness of personal information security of academic and administrative staff working in universities will contribute positively to ensuring corporate information security. In addition, it can be said that encouraging formal communication within the institution will positively affect the provision of corporate information security. Promoting organizational knowledge sharing by increasing formal communication within the institution will positively contribute to the provision of corporate information security.

Keywords: Information security, corporate information security, organizational communication, organizational knowledge sharing.

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

EKLER LİSTESİ

SİMGELER VE KISALTMALAR

Simgeler

χ^2 : Ki Kare

$\bar{X}$: Ortalama

Kısaltmalar

YEM	: Yapısal Eşitlik Modeli
AFA	: Açımlayıcı Faktör Analizi
DFA	: Doğrulayıcı Faktör Analizi
ANOVA	: Varyans Analizi

1. GİRİŞ

Teknolojide yaşanan gelişmeler, bilgi varlıklarının artmasına, günümüzün bilgi çağı olarak nitelendirilmesine neden olmuştur. Günümüzde bilgi giderek daha fazla önem kazanmaya başlamıştır. Bu bağlamda bilgi fikirlerin, kuralların, prosedürlerin ve enformasyonun organize edilmiş bir birleşimi olarak tanımlanmaktadır (Bhatt, 2000: 16). Enformasyonun deneyim, bağlam, yorum ve yansımayla birleştirilmesi sonucu ortaya çıkan (Davenport ve Prusak, 1998: 3) bilgi, kuruluşların daha iyi kararlar almalarına ve daha iyi hizmetler sunmalarına yardımcı olmaktadır (Tu, Yuan, Archer ve Connelly, 2018: 150). Örgütsel bağlamda bilginin amacı, kurum ve tüm paydaşlar için değer yaratmak veya var olan değeri arttırmaktır (Liew, 2007: 5). Kurumun sahip olduğu diğer varlıklar gibi bilginin de en iyi biçimde korunması gerekmektedir (Kahraman, 2006: 1; Lebek, Uffen, Breitner, Neumann ve Hohler, 2013: 2978; Demirok, 2016: 1). Bu bağlamda kurumlar için bilgi güvenliği büyük önem kazanmaktadır (Da Veiga, Astakhova, Botha ve Herselman, 2020: 1; Vroom ve Von Solms, 2004: 191). Bilgi güvenliği, bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini koruma çalışması ve uygulaması olarak tanımlanmaktadır (Grama, 2020: 13). Bilginin yetkisiz erişim, kullanım, ifşa, bozulma, değişiklik veya imhaya karşı korunmasını (Cebula ve Young, 2010: 10) sağlama disiplini olarak görülen bilgi güvenliği, günümüzde herhangi bir kurumun stratejik yönetimi için önemli konular arasında yer almaktadır (Von Solms, 2001: 215; Eslamkhah ve Seno, 2019: 1; Soliman ve Mohammadnazar, 2022: 6818).

Bilgi güvenliğinin temel amacı bir kurumun bilgilerini korumaktır (François, 2016: 4). Teknolojinin gelişmesiyle kurumlar bilişim teknolojilerini veri işleme, depolama ve aktarma gibi çeşitli şekillerde kullanmaktadır (Mahabi, 2010: 1). Bilişim teknolojilerinde yaşanan gelişmeler kurumlar için pek çok fırsat sunmasına rağmen aynı zamanda bilgi güvenliği açısından da birçok riski beraberinde getirmektedir (Vroom ve Von Solms, 2004: 191; Gencer, 2015: 1; Eslamkhah ve Seno, 2019: 1). Bilgi güvenliğine yönelik artan tehditler kurumlar için büyük endişe oluşturmaktadır (Jones, 2009: 121). Ayrıca bilgi güvenliği bilişim uzmanlarının karşılaştığı en rahatsız edici konular arasında yer almaktadır (AlKalbani, Deng ve Kam, 2014: 2). Kurumları farklı güvenlik saldırılarına karşı korumak için güvenlik önlemleri uygulanmaktadır (Alshboul, 2010: 2).

Kurumsal bilgi güvenliğinin sağlanmasında teknolojik, örgütsel ve bireysel özellikler etkilidir (Von Solms ve Von Solms, 2004: 373; Chang ve Ho, 2006: 347; Hu, West ve Smarandescu, 2015: 7). Kurumsal bilgi güvenliğinin başarılı bir biçimde sağlanması için bilgi güvenliğinin teknik, yönetim ve insani yönlerinin dengeli bir yapıya sahip olması gerekmektedir (Narain Singh, Gupta ve Ojha, 2014: 644). Bilgiyi korumak için birçok teknoloji türü mevcuttur (Colwill, 2009: 187). Teknik yöntemler, şifreleme, güvenlik duvarları, güçlü kimlik doğrulama yöntemleri ve güvenlik modelleri, bilgi sistemlerinin güvenlik saldırılarına karşı korunmasında etkili olmaktadır (Colwill, 2009: 187; Mahabi, 2010: 12). Kuruluşların bilgi varlıklarının gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak için modernize edilmiş yöntemler ve sistemler geliştirilmeye ve kullanılmaya devam etmektedir (Antoniou, 2015: 7). Ancak yapılan araştırmalar, bilgi güvenliğinin sağlanmasında sadece teknolojik önlemlerin alınmasının yeterli olmadığını (Vardal, 2009: 3), bilgi güvenliğinde en zayıf halkanın insan olduğunu vurgulamaktadır (Bulgurcu, Çavuşoğlu, Benbasat, 2010: 524; Hua ve Bapna, 2013: 48; Pfleeger, Sasse ve Furnham, 2014: 4).

Bir kurumu bilgi güvenliği açısından riske sokabilecek insan davranışları, yanlışlıkla veya kasıtlı olarak şifreleri başkalarına ifşa etme, gömülü web sitesi bağlantılarına tıklayarak veya tanıdık olmayan medyayı iş veya ev bilgisayarlarına ekleyerek kimlik avı e-postalarına maruz

kalma gibi davranışları içermektedir (Parsons, McCormac, Butavicius, Pattinson ve Jerram, 2014: 165). Kurum çalışanlarının bireysel bilgi güvenliğine sahip olmaması, kuruma verilecek zararında farkında olmamalarına neden olmaktadır (Von Solms ve Von Solms, 2004: 372). Bilgi güvenliği farkındalığına sahip çalışanlar, kurumsal bilgi güvenliğinin sağlanmasına katkıda bulunabilirler (Gyllensten ve Torner, 2021: 15). Kurumsal bilgi güvenliğinin sağlanması, kullanıcıların ve diğer paydaşların (yöneticiler, uygulayacılar, politika üreticileri, teknik çalışanlar vb.) güvenlik analizi, tasarım ve uygulama süreçlerine ve bilgi yönetimine aktif bir şekilde katılımıyla ilişkilidir (Belsis, Kokolakis ve Kiountouzis, 2005: 190). Bu bağlamda kurumun örgütsel yapısı ve örgütsel bilgi güvenliği farkındalığı kurumsal bilgi güvenliğinin sağlanmasında etkili unsurlar arasında yer almaktadır (Furnell ve Rajendran, 2012: 13; Kraemer, Carayon ve Clem, 2009: 509). Bir kurumun örgütsel yapısı örgütsel iletişimle yakından ilişkilidir. Örgütsel iletişim, genellikle bireylerin ve grupların amaçlarının yerine getirilmesi amacıyla örgüt içindeki bireyler, gruplar ve örgütsel seviyeler arasında mesaj alışverişinde bulunma amaçlı bir süreç olarak tanımlanmaktadır (Andrioni ve Popp, 2012: 591). Bir kuruluşun başarısı veya başarısızlığında önemli bir etkiye sahip olan örgütsel iletişim (Mitrofan ve Bulborea, 2013: 511) kurumsal bilgi güvenliğinin sağlanmasında göz ardı edilmemelidir (Arhin ve Wiredu, 2018: 275). Bir kurumda örgütsel iletişim formel ve informel biçimde gerçekleşebilir. Formel iletişim, önceden planlanmış, genellikle gündemi önceden belirlenmiş, kurumun resmi çalışmasına ilişkin mesaj alışverişidir (Kraut, Fish, Root ve Chalfonte, 1990: 5; Lunenburg, 2010: 2). İnformel iletişim ise planlanmamış, belirli bir gündemi olmayan, gayri resmi bir dil kullanılabilen iletişim türüdür (Kraut vd. 1990: 5).

Örgüt içerisindeki bilgi paylaşımı da bir iletişim biçimidir ve iletişim bilgi paylaşımını etkilemektedir (Van Den Hooff ve De Ridder, 2004: 121,126). Bilgi paylaşımı, örgüt içerisinde veya örgütler arasında bilginin transferi ve akışının sağlanması olarak tanımlanmaktadır (Erden, 2016: 28). Bireysel ve örgütsel öğrenmeye katkıda bulunan bilgi paylaşımı, bilgi edinmeyi ve bilgi dağıtımını içeren bir süreçtir (Akgün, Keskin ve Günsel, 2009: 183). Kurumsal bilgi güvenliğini başarılı bir şekilde gerçekleştiren kurumlarla işbirliği ve bilgi paylaşımı yapılması kurumsal bilgi güvenliğini sağlamada kolaylık sağlayabilmektedir (Von Solms ve Von Solms, 2004: 375). Güvenlik olaylarına müdahale etmek, politika geliştirmek, güvenlik ihlallerini rapor etmek gibi bilgi güvenliği alanındaki bilgi paylaşımı bilgi güvenliği işbirliğinin örnekleri arasında yer almaktadır (Safa, Von Solms ve Futcher, 2016: 16). Bilgi güvenliği alanında deneyimlerin paylaşılması, bilgi güvenliği bilincinde değerli bir kaynak olarak görülmektedir (Wall ve Palvia, 2021: 436; Safa vd., 2016: 17). Ayrıca bilgi güvenliği farkındalığı üzerinde olumlu etkilere sahip olan bilgi paylaşımı, kurumsal bilgi güvenliğinde önemli bir etkiye sahiptir (Kampanakis, 2014: 42). Çalışanlar arasında etkin bilgi güvenliği bilgi paylaşımı sadece etkin bir yaklaşım olarak farkındalık seviyesini arttırmaz, aynı zamanda kurumlarda bilgi güvenliği maliyetini de düşürmektedir (Safa vd., 2016: 16). Bilgi paylaşımının kurum için katkılarının öneminin giderek anlaşılmasına rağmen bilginin doğası bilgi paylaşımını etkilemektedir (Yao, Crupi, Di Minin ve Zhang, 2020: 608). Bilgi doğası gereği örtük ve açık bilgi şeklinde paylaşılmaktadır (Flores, Antonsen ve Ekstedt, 2013: 93). Açık bilgi, somut veriler, bilimsel formüller gibi kolayca iletilebilen ve paylaşılabilen bilgi türü iken örtük bilgi ise kodlanmamış, biçimlendirilmemiş, kişisel ve resmileştirmesi zor olan bilgi türüdür (Nonaka ve Takeuchi, 1995: 8; Akgün vd., 2009: 23). Açık bilginin pratik kullanımı, örtük bilginin uygun şekilde paylaşılması ve kullanılması ile mümkündür (Salameh ve Zamil, 2020: 2230). Örtük ve açık bilgi örgüt içerisinde formel veya informel yollarla paylaşılmaktadır (Yao vd., 2020: 621).

İlgili alan yazında kurumsal bilgi güvenliğinin başarısını etkileyen kritik faktörlerin keşfedilmesi, kurumsal bilgi güvenliğinin başarısını sağlayan mekanizmaların tespit edilmesi gerekliliği vurgulanmaktadır (Tu vd., 2018: 151). Ayrıca kurumsal bilgi güvenliğinin insani yönüyle ilgili çalışmalar, bireysel bilgi güvenliği düzeyine veya örgütsel faktörlere odaklanılan çalışmalar yapılmaktadır. Ancak örgütsel ve bireysel faktörlerin birlikte incelenmesi gereken çalışmalara ihtiyaç duyulmaktadır (Flores vd., 2013: 92). Bu bağlamda tez çalışmasının amacı üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliğinin, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı bağlamında değerlendirilmesidir.

1.1. Araştırmanın Problemi

Kurumsal bilgiler, kuruma rekabet avantajı, doğru strateji belirleme, başarılı bir iş/ çalışma sürecinin yaşanması gibi birçok avantaj sağlamaktadır. Bu nedenle kurumsal bilgiler günümüzde çoğu organizasyonda son derece önemli bir rol oynamaktadır ve kurumsal bilgilerin korunması için yoğun çaba harcanmaktadır (Posthumus ve Von Solms, 2004: 638). Teknolojik önlemlerin alınmasına rağmen bilgi güvenliğine yönelik ihtiyaç artmakta ve bilgi güvenliği ciddi bir sorun olmaya devam etmektedir (Narain Singh vd. 2014: 644). Virüsler, oltalama, çalınan şifreler ve sosyal mühendislik kurumların karşılaştığı riskler arasında yer almakta ve bu risklerin tümü kuruluşun işleyişine zarar vermektedir (Mahabi, 2010: 11-12). Önceki çalışmalar bilgi güvenliği ve gizlilik ihlallerinin, kurumlar ve insanlar için önemli konular arasında olduğunu göstermektedir (Safa vd., 2019: 588). Araştırmalar teknolojik önlemlerin, çoğu zaman kurumsal bilgi güvenliği ile ilgili sorunlara tek çözüm olamayacağını bulgulamıştır (Hadlington, Popovac, Janicke, Yevseyeva ve Jones, 2019: 41). Yapılan araştırmalar bilgi güvenliğine ilişkin insan faktörlerine de odaklanılması gerektiğini vurgulamaktadır (Mahabi, 2010: 14; Hadlington vd., 2019: 42). Benzer bir çalışmada, Rezgui ve Marks (2008: 250) insan faktörlerinin, örgüte yönelik tutumun, personel davranışlarının bilgi güvenliğini etkilediğini belirtmiştir. Ancak bilgi güvenliğinin örgütsel ve bireysel yönleri çoğu zaman kurumlar tarafından göz ardı edilmektedir (Narain Singh vd. 2014: 649).

Alan yazın incelendiğinde kurumsal bilgi güvenliğinin teknik olmayan boyutlarının araştırılmaya (Lee, 2015: 4; Safa ve Von Solms, 2016: 442; Çatuk, 2018: 4; Sauerwein, Pekaric, Felderer ve Breu, 2019: 140) başlandığını ancak örgütsel iletişim rolünün yeterli düzeyde araştırılmadığı görülmektedir (Arhin ve Wiredu, 2018: 262). Kurumsal bilgi güvenliğinin örgütsel iletişim boyutunun da incelendiği çalışmalara ihtiyaç duyulduğu vurgulanmaktadır (Arhin ve Wiredu, 2018: 262). Ayrıca örgütsel iletişim bilgi paylaşımı ile yakından ilişkilidir ve örgüt içerisindeki iletişim biçimleri bilgi paylaşımını etkilemektedir (Ramayah, Yeap ve Ignatius, 2014; Hwang, 2020: 2; Salameh ve Zamil; 2020: 2230). Örgüt içerisindeki etkili bilgi paylaşımı etkili bir iletişim gerektirmektedir (Hwang, 2020: 2).

Yükseköğretim kurumları akademik, araştırma ve idari faaliyetleri için bilgisayar sistemlerini ve bilgi işlem süreçlerini kullanmaktadır (Rezgui ve Marks, 2008: 241). Diğer kurumlarla aynı stratejik ve karar verme türlerine ilişkin bilgilerin yanı sıra yükseköğretim kurumları öğretme, öğrenme ve araştırma bilgilerine de sahiptir (Waddell, 2013: 1). Üniversiteler, bilginin üretilmesi, dağıtılması, sunulması ve taşınmasında öncü kuruluşlar arasında yer almaktadır (Keser ve Güldüren, 2015: 1169). Sahip olduğu yoğun bilgiler nedeniyle üniversiteler siber saldırıların hedefinde yer almaktadır (Waddell, 2013: 2). Yükseköğretim kurumları, önemli

miktarda bilgi varlıklarına sahip olması nedeniyle bilgi güvenliğinin ve bütünlüğünün sağlanması için yüksek teknoloji altyapısına büyük yatırım yapmaktadırlar (Rajab ve Eydgahi, 2019: 212).

Üniversitelerde görev yapan akademik ve idari personel, kurumsal bilgi güvenliğinin sağlanmasındaki insan faktörünü oluşturmaktadır (Aslan Öztezcan, 2017: 3). Yükseköğretim kurumlarında çalışan akademik ve idari personelin, yükseköğretim kurumlarının karşılaştığı güvenlik tehditlerinin ve zorluklarının farkında olması, üniversitelerin sahip olduğu bilgi ve bilgi varlıklarının potansiyel olarak kaybedilmesini önlemek için gerekli görülmektedir (Waddell, 2013: 2). Bu nedenle üniversite personelinin bilgi güvenliğini ön planda tutması ve bu konuya özen göstermesi gerekmektedir (Keser ve Güldüren, 2015: 1169). Ayrıca üniversiteler bilgi yaratma, bilgi yayma ve uygulama çalışmalarının merkezde olduğu kurumlardır (Mutahar vd., 2022: 3). Bu nedenle üniversitede çalışan personel farklı türlerde bilgi paylaşımında bulunabilmektedirler (Fullwood, Rowley ve McLean, 2019: 130).

Üniversitelerin sahip olduğu önemli kurumsal bilgiler, bilgi güvenliği ihlallerinin kurumlara verdiği zararlar, örgütsel iletişim ve bilgi paylaşımının kurumsal bilgi güvenliğini sağlamada önemli etkenler arasında yer alması, kurumsal bilgi güvenliğinin sağlanmasında örgütsel iletişim ve bilgi paylaşımı ile ilgili yeterli çalışmaya rastlanmaması bu araştırmanın ortaya çıkış sebepleri arasında yer almaktadır. Bu çalışma ile zengin bilgi kaynaklarına sahip olan üniversitelerin, kişisel bilgi güvenliği farkındalığının, örgütsel iletişimin ve örgütsel bilgi paylaşımının kurumsal bilgi güvenliği üzerindeki etkilerini inceleyerek alana katkı sağlayacağı düşünülmektedir.

1.2. Araştırmanın Amacı

Kurumun değerli varlıkları arasında yer alan bilgi, kurum içinden ve dışından gelen tehditlere açıktır (Jones, 2009: 121). Kurumun sahip olduğu bilgileri korumak için sadece teknolojik önlemler alınmasının yeterli olmadığı, bilgi güvenliğinin sağlanması için örgütsel ve bireysel önlemlerin alınması gerektiği vurgulanmaktadır (Vardal, 2009: 3; Johnson ve Goetz, 2007: 17). Çalışanların bilgi güvenliği farkındalığı ve davranışı kurumsal bilgi güvenliği performansının önemli bir parçasıdır (Albrechtsen ve Hovden, 2010: 432). Aynı zamanda kurumsal bilgi güvenliğinin sağlanmasında çalışanların bilgi güvenliği davranışları ve kurumun örgütsel yapısının etkili olduğu belirlenmiştir (Johnson ve Goetz, 2007: 17; Ramachandran, 2007: 2; Tu vd., 2018: 155). Bilgi güvenliği ihlallerinin önlenmesi veya bu ihlallere cevap verebilmek için kurumsal işbirliğinin (Arhin ve Wiredu, 2018: 262), bilgi paylaşımının (Kampanakis, 2014: 42), çalışanların katılımının (Johnson ve Goetz, 2007: 23) sağlanması değerli görülmektedir. Alan yazın incelendiğinde, araştırmacılar çalışanların bilgi güvenliğine nasıl ve niçin uymadıklarına (Hadlington vd., 2019: 42), bilgi güvenliğini etkileyen örgütsel ve bireysel faktörlerin belirlenmesine (Safa vd., 2016: 18; Haeussinger ve Kranz, 2017: 1; Tu vd., 2018: 163) yönelik araştırmaların yapılmasını önermektedirler. Bu bağlamda, gerçekleştirilen araştırmada üniversitelerde görev yapan akademik ve idari personelin kurumsal bilgi güvenliğinin, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı bağlamında değerlendirilmesi amaçlanmıştır.

Bu amaca yönelik olarak aşağıdaki araştırma sorularına cevap aranmaktadır.

1. Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliğine, kişisel bilgi güvenliği farkındalığına, örgütsel iletişime ve örgütsel bilgi paylaşımına ilişkin algıları ne düzeydedir?
2. Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı demografik

değişkenlere (cinsiyet, yaş, hizmet süresi, İnternette/ sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı) göre anlamlı farklılık göstermekte midir?

3. Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği ile kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı arasında nasıl bir ilişki vardır?
4. Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliğinin veri madenciliği yöntemleri ile tahmin başarımı nedir?

Elde edilen bulgulardan hareketle bu çalışma sonucunda, üniversitelerde görev yapan akademik ve idari personele, bilişim uzmanlarına kurumsal bilgi güvenliğini etkileyen etmenler açısından önerilerde bulunulması hedeflenmektedir.

1.3. Araştırmanın Önemi

Örgütün sahip olduğu bilgiye karşı yapılan saldırılar kurumlar için ciddi kayıplara neden olmaktadır (Arhin ve Wiredu, 2018: 261). Alan yazında kurumsal bilgi güvenliğinin sağlanması amacıyla çeşitli bilgi güvenliği yönetim sistemi araçlarının geliştirildiği belirlenmiştir (Çetinkaya, 2008: 11; Kandemirli, 2012: 5). Ancak kurumlar bilgi güvenliğini sağlamak amacıyla teknik olmayan önlemler almaya da başlamışlardır (Arhin ve Wiredu, 2018: 262; Eslamkhah ve Seno, 2019: 1).

Kurumsal bilgi güvenliğinin sağlanmasında örgüt yapısı ve bireysel iletişim özellikleri dikkate alınması gereken kritik faktörler arasında yer almaktadır (Chan, Woon ve Kankanhalli, 2005; Ramachandran, 2007: 3; Arhin ve Wiredu, 2018: 262; Tu vd., 2018: 153). Benzer bir çalışmada Von Solms ve Von Solms, (2004: 372), kurumsal bilgi güvenliğinin sağlanması için örgütsel yapının, kişisel bilgi güvenliği farkındalığının dikkate alınması gerektiği vurgulanmaktadır. Bulgurcu vd. (2010: 526), kurumsal bilgi güvenliğinin sağlanması için örgütsel ve bireysel özelliklerin birlikte araştırılması gerektiğini belirtmişlerdir. Çalışanların bilgi güvenliği bilinci, bilgi güvenliği ihlallerinin riskini azaltmada önemli faktörler arasında yer aldığı kabul edilmektedir (Parsons vd.,2014: 166; Safa ve Von Solms, 2016: 443). Diğer bir deyişle çalışanların bilgi güvenliği davranışları kurumsal bilgi güvenliğini etkilemektedir (Ramachandran, 2007: 3). Çalışanların bilgi güvenliği bilinci, gelişen bir araştırma alanıdır ve kuruluşları siber saldırılara ve bilgi güvenliği olaylarına karşı korumada kilit bir rol oynamaktadır (Haeussinger ve Kranz, 2017: 1).

Ayrıca kurumsal bilgi güvenliğinin sağlanmasında, kurumun bilgi güvenliğinin insani yönleri olan bilgi paylaşımı, bilgi güvenliği işbirliği, bilgi güvenliği bilinci davranışlarının dahil edilmesi vurgulanmaktadır (Safa vd., 2016: 16). Bilgi paylaşımı örgütsel işbirliğini arttırmakta ve bunun sonucu olarak bilgi güvenliği ihlalleri riskini azaltmakta etkili olmaktadır (Parsons vd, 2014: 166). Çalışanların bilgi güvenliği konusundaki farkındalığı üzerindeki olumlu etkisi nedeniyle bilgi paylaşımı, bilgi güvenliği alanında önemli bir rol oynamaktadır (Safa ve Von Solms, 2016: 443). Ancak alan yazın incelendiğinde Dünya'da ve Türkiye'de yapılan çalışmalar farkındalık eğitimleri, bilgi güvenliği sorunlarına yönelik durum tespiti, bilgi güvenliği risk değerlendirmeleri ve bilgi güvenliği yönetim sistemleri konu başlıkları altında toplandığı belirlenmiştir (Keser ve Güldüren, 2015: 1169). Benzer bir biçimde alan yazın incelendiğinde, kurumsal bilgi güvenliğinin sağlanmasında, örgütsel iletişimin rolünün yeterince araştırılmadığı vurgulanmıştır (Arhin ve Wiredu, 2018: 277). Kurumsal bilgi güvenliğinin sağlanabilmesi için örgütsel faktörlerin

çalışanların bilgi güvenliği davranışlarını nasıl etkilediğinin araştırılması önerilmektedir (Siponen, Pahnila ve Mahmood, 2010: 70; AlKalbani, Deng ve Kam, 2019: 157). Benzer bir çalışmada ise Hadlington ve arkadaşları (2019: 43) bilgi güvenliği bağlamında çalışanların potansiyel risk faktörleri hakkında ayrıntılı bilgi sahibi olmanın, araştırmacılara ve güvenlik uygulayıcılarına bilgi güvenliği için kapsamlı bir çerçeve geliştirmelerine yardımcı olabileceğini belirtmektedir.

Bu bağlamda bilginin üretiminde, öğretiminde, dağıtımında öncü kurumlardan olan üniversitelerde görev yapan akademik ve idari personelin kurumsal bilgi güvenliğinin, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı bağlamında değerlendirilmesi önemli görülmektedir. Tez çalışmasında, kişisel bilgi güvenliğinin, kişisel bilgilerin korunması ile saldırı ve tehditler boyutlarıyla derinlemesine araştırılması ve kurumsal bilgi güvenliği ile ilişkisinin belirlenmesi faydalı olacaktır. İlgili alan yazında çoğu çalışmanın örgütsel iletişimi genel olarak incelemesine rağmen bu çalışmada örgütsel iletişim, formel ve informel iletişim olarak incelenmesinin alana katkı sağlayacağı düşünülmektedir. Benzer şekilde bilgi paylaşımının örtük ve açık bilgi paylaşımı olarak araştırılması önemli görülmektedir. Ayrıca bu çalışmada kurumsal bilgi güvenliğinin formel ve informel iletişim, açık ve örtük bilgi paylaşımı açısından detaylandırılarak değerlendirilmesi, kişisel bilgi güvenliği farkındalığının da incelenmesi ilgili alan yazında yer alan diğer çalışmalardan farkı olarak değerlendirilmekte ve alana katkı sağlayacağı düşünülmektedir. Bu çalışmada veri madenciliği yöntemleri de kullanılmıştır. Farklı analiz yöntemlerinin bir arada kullanılması ve sonuçlarının karşılaştırılması önemli görülmüştür.

1.4. Araştırmanın Sayıltıları (Varsayımları)

- Katılımcılar bilgi güvenliği, bilgi güvenliği farkındalığı, örgütsel iletişim ve bilgi paylaşımı ölçeklerini gönüllülük esasına göre içtenlikle cevaplamıştır.
- Ölçme formuyla elde edilen bilgiler, örneklemde yer alan akademik ve idari personelin görüşlerini yansıtmaktadır.

1.5. Araştırmanın Sınırlılıkları

Bu tez çalışması aşağıdaki sınırlılıklar çerçevesinde planlanıp, gerçekleştirilmiştir:

- Bu çalışma Türkiye'nin doğusunda yer alan bir üniversitede görev yapan akademik ve idari personel ile sınırlıdır.
- Kurumsal bilgi güvenliğini etkileyen çeşitli etmenlerden kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı ile sınırlıdır.
- Bu çalışma Türkiye'nin doğusunda yer alan bir üniversitede görev yapan akademik ve idari personelin ölçeklere verdikleri yanıtlar ile sınırlıdır.
- Araştırma, ölçeklerin geçerlik ve güvenirlikleri ile sınırlıdır.

1.6. Araştırmanın Tanımları

Bilgi Güvenliği: Bilgi güvenliği, yetkisiz erişim, ifşa, kullanım, değişiklik, aksaklıktan bilgileri korumaktır (Safa ve Von Solms, 2016). Uluslararası standart olan ISO/IEC 27002 (2005), bilgi güvenliğini bilgilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması olarak tanımlamaktadır.

Örgütsel İletişim: Örgütsel iletişim, örgütün işleyişi ve amaçlarına ulaşması amacıyla örgüt içerisindeki birimler ve örgütün çevresi ile arasındaki iletişim ve bilgi alışverişini sağlayan sosyal

bir süreçtir (Blazenaite, 2011: 87). Yönetimsel, kişiler arası ve diğer iletişim biçimleri dahil olmak üzere örgütsel iletişim, kuruluş genelinde politikalar, stratejiler, talimatlar ve bilgiler taşımaktadır (Gochhayat, Giri ve Suar, 2017: 693).

Formel İletişim: Çalışanların işle ilgili hedeflere ulaşmak için profesyonel rollerine göre etkileşimde bulunmaları şeklinde tanımlanmaktadır. Formel iletişim, yüz yüze ve sanal toplantılar, raporlar, metin tabanlı konuşmalar ve telefon görüşmeleri gibi birçok iletişim kanalı kullanılarak gerçekleştirilebilir (Koch ve Denner, 2022).

İnformel İletişim: Çalışanların birbirleri ile profesyonel rolleri dışında etkileşimde bulunmalarıdır (Koch ve Denner, 2022).

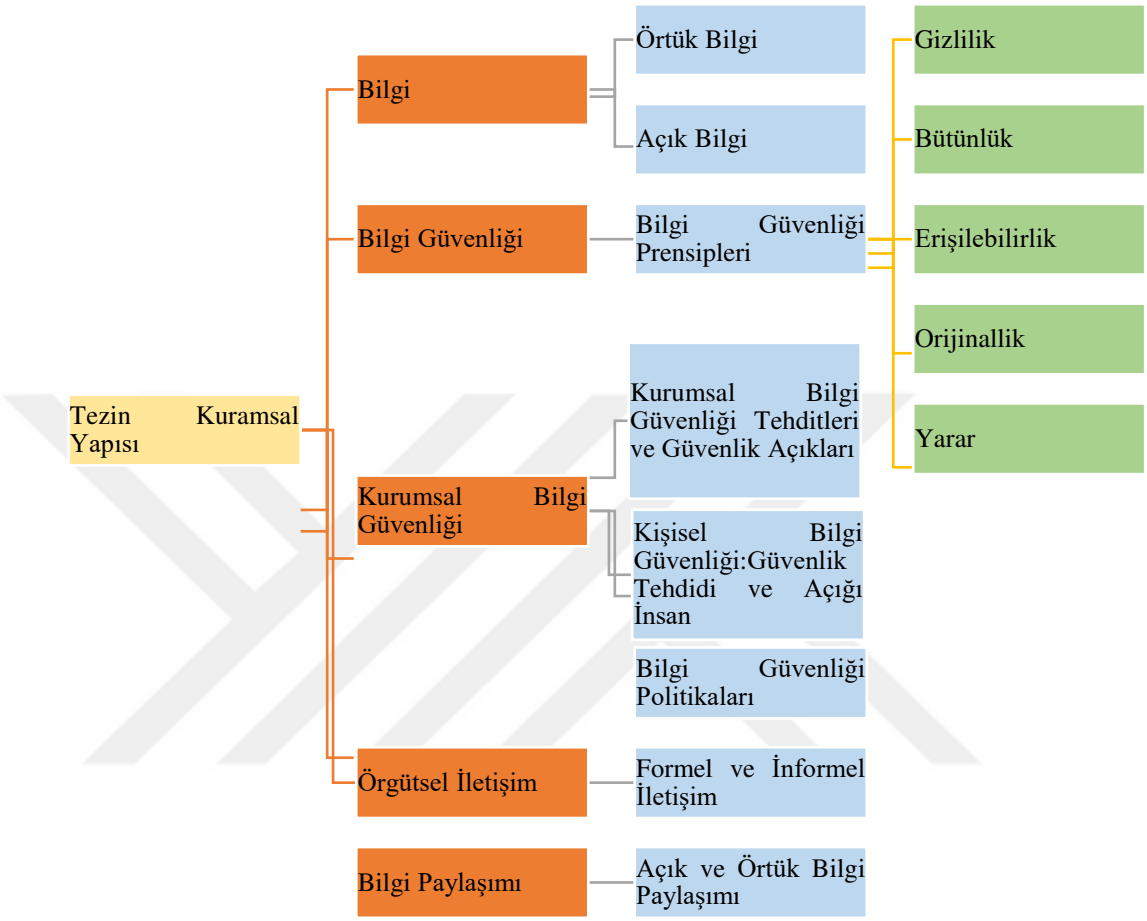
Örgütsel Bilgi Paylaşımı: Bilgi paylaşımı, bireyler, gruplar ve kuruluşlar arasındaki bilgi alışverişi olarak tanımlanmaktadır (King ve He, 2011: 914).

Açık Bilgi Paylaşımı: Somut veriler, formüller, kelimeler ve sayılarla ifade edilebilen açık bilgi, kolayca ve tamamen paylaşılabilmektedir (Nonaka ve Takeuchi, 1995: 8).

Örtük Bilgi Paylaşımı: Kodlanmamış, somut olmayan örtük bilgi, yapılandırılmamış veya yarı yapılandırılmış şekilde paylaşılmaktadır (Howells, 1996: 92).

2. KURAMSAL ÇERÇEVE VE İLGİLİ ALAN YAZIN

Tez çalışması ile ilgili kuramsal çerçeve bilgi, bilgi güvenliği, kurumsal bilgi güvenliği, örgütsel iletişim, bilgi paylaşımı, eğitsel veri madenciliği başlıkları altında incelenmiştir. Kuramsal çerçeve açısından incelenen başlıklar ve alt başlıklar Şekil 1'de sunulmuştur.



Şekil 1. Tezin Kuramsal Çerçevesi

2.1. Bilgi

Bilgi kavramı, tanımlanırken veri ve enformasyon kavramıyla açıklanmaktadır. Veri, enformasyon ve bilgi kavramları genellikle birbirlerinin yerine kullanılmalarına rağmen aslında aralarında açık ayrımlar bulunmaktadır (Nonaka ve Takeuchi, 1995: 57) ve birbirinden farklı şeylerdir (Boisot ve Canals, 2004: 44). Bu bağlamda bilgi kavramını tanımlamak için öncelikle veri ve enformasyon kavramlarını tanımlamak gerekmektedir.

Veri, nesnelerin ve olayların özelliklerini temsil eden sembollerdir (Ackoff, 1989: 4) ve veriler hamdır yani işlenmemiştir (Bellinger, Castro ve Mills, 2004: 1). Veriler, kullanılabilir olsun veya olmasın herhangi bir biçimde olabilir ve yalnız başına bir anlam ifade etmemektedir (Bellinger vd. 2004: 1). Veri, enformasyon ve bilgiye temel teşkil etmektedir (Yılmaz, 2009: 4).

Enformasyon işlenmiş verilerden oluşur, elde edilen verilerin işlenmesi kullanışlılığı arttırmaya yönelik bir çalışmadır. Nesnelerin ve olayların özelliklerini temsil eden enformasyon, bunu derli toplu ve kullanışlı bir şekilde yapmaktadır. Yani enformasyonda kim, ne, ne zaman,

nerede ve kaç gibi soruların cevaplarının yanıtı yer almaktadır (Ackoff, 1989: 4). Benzer bir ifadeyle enformasyon, olayları veya nesneleri yorumlamak için yeni bir bakış açısı sağlamakta, bu da önceden görünmeyen anlamları görünür kılmakta veya beklenmedik bağlantılara ışık tutmaktadır. Dolayısıyla enformasyon, bilgiyi ortaya çıkarmak ve inşa etmek için gerekli bir ortam veya malzemedir (Nonaka ve Takeuchi, 1995: 58).

Bilgi genellikle zengin bir enformasyon biçimi olarak görülmektedir. Ancak bu ayrım çokta yeterli değildir (Gurteen, 1999: 1). Enformasyon bir mesaj akışıdır, bilgi ise sahibinin inançlarına ve değerlerine bağlı olarak bu enformasyon akışı tarafından oluşur (Nonaka ve Takeuchi, 1995: 59). Bu bağlamda bilgi, enformasyonun deney, tecrübe veya yorumla bir araya gelerek oluşan; kişisel anlamda düzenlenmiş enformasyon olarak tanımlanabilir (Aktan ve Vural, 2016: 8). Bilgi enformasyondan farklı olarak eylemle ilgilidir (Nonaka ve Takeuchi, 1995: 46) ve enformasyonu uygulamaya geçirebilme yeteneğidir (Liebowitz ve Megbolugbe, 2003: 190). Polanyi (1966, Aktaran: Akgün vd., 2009: 22) ilk kez bilgiyi açık ve örtük bilgi olarak sınıflandırmıştır. Açık ve örtük bilgi ayrı başlıklar altında incelenmiştir.

2.1.1. Kaynağına Göre Bilgi Türleri

Bilgi kaynağına göre örtük ve açık bilgi olarak ikiye ayrı başlık altında incelenmektedir.

2.1.1.1.Örtük Bilgi

Örtük bilgi, biçimsel olmayan yollarla öğrenilen; biçimlendirilmemiş, kodlanmamış bilgi çeşidi olarak tanımlanmaktadır (Akgün vd., 2009: 23). Kişisel ve resmileştirilmesi zor olması nedeniyle paylaşılması zor olan bilgi türüdür (Nonaka ve Takeuchi, 1995: 8). Benzer bir ifadeyle kişisel olan örtük bilginin ifade edilmesi zordur ve deneyimlere dayanmaktadır (Small, 2005: 13). Chilton ve Bloodgood (2008: 79), örtük bilginin temelde dört temel unsura dayandırarak açıklamışlardır. Bu unsurlar,

- Örtük bilgi kullanıldığında, kullanıcı bilinçli olarak bunun farkında değildir diğer bir deyişle örtük bilgide bilinçli farkındalık eksiktir,
- Örtük bilgiyi başkalarına ifade etmek zordur,
- Örtük bilginin ispatlanması zordur,
- Kişinin resmi veya gayri resmi önceki öğrenmeleriyle ilişkilidir.

Öznel iç görüler, sezgiler ve önseziler örtük bilgi olarak ifade edilirken aynı zamanda örtük bilgi, bir bireyin eylem ve deneyiminin yanı sıra benimsediği idealler, değerler veya duygular olarak da kabul edilir (Nonaka ve Takeuchi, 1995: 8). Örtük bilgi iki boyuta bölünebilir. Birincisi, "know-how" terimiyle yakalanan gayri resmi ve tespit edilmesi zor becerileri veya zanaatları kapsayan teknik boyuttur. Örneğin usta bir zanaatkar, yılların deneyiminden sonra "parmaklarının ucunda" zengin bir uzmanlık geliştirmesidir. Ancak bildiklerinin arkasındaki bilimsel veya teknik ilkeleri genellikle ifade etmesi zordur. İkincisi ise örtük bilgi önemli bir bilişsel boyut içermektedir. Örtük bilgi şemalardan, zihinsel modellerden, inançlardan ve algılardan oluşur. Örtük bilginin bilişsel boyutu, gerçeklik imajımızı (ne olduğunu) ve gelecek vizyonumuzu (ne olması gerektiğini) yansıtmaktadır. Çok kolay ifade edilememelerine rağmen, bu örtük modeller çevremizdeki dünyayı algılama şeklimizi şekillendirmektedir (Nonaka ve Takeuchi, 1995: 8). Örtük bilginin öznel ve sezgisel doğası nedeniyle örgüt içerisinde sistematik veya mantıksal şekilde işlenmesini veya aktarılmasını zorlaştırmaktadır (Nonaka ve Takeuchi, 1995: 9). Bu nedenle örgüt içerisinde örtük

bilginin öğrenilmesi ve paylaşılabilmesi için bire bir çalışma, mentör, stajlar, iş başında eğitim, beyin fırtınası gibi fırsatlar oluşturulmalıdır (Smith, 2001: 314). Örtük bilginin kuruluş içinde iletilmesi ve paylaşılması için herkesin anlayabileceği kelimelere veya sayılara dönüştürülmesi gerekmektedir (Nonaka ve Takeuchi, 1995: 9) Ayrıca yüz yüze iletişim, video konferans, sohbet, hikaye anlatımı gibi etkinliklerle örtük bilginin paylaşılması sağlanabilir. Örgüt içerisinde örtük bilginin paylaşılması için çalışanların yaratıcılıkları desteklenebilir, motive edici ödüller verilebilir (Smith, 2001: 314).

2.1.1.2.Açık Bilgi

Açık bilgi, kelimeler ve sayılarla ifade edilebilen, somut veriler, bilimsel formüller, kodlanmış prosedürler veya evrensel ilkeler şeklinde kolayca iletilebilen ve paylaşılabilen bilgi türü olarak tanımlanabilir (Nonaka ve Takeuchi, 1995: 8). Açık bilgi, tamamen aktarılabilirdir ve kullanıcılar bilinçli olarak kullanımının farkındadır (Chilton ve Bloodgood, 2008: 79). Aynı zamanda açık bilgi bir bilgisayar tarafından kolaylıkla "işlenebilir", elektronik olarak iletilebilir veya veri tabanlarında depolanabilir (Nonaka ve Takeuchi, 1995: 9). Kişinin neyi bildiği yani "know-what" ile ilişkilidir (Smith, 2001: 315), resmi ve sistematiktir ayrıca genellikle kitaplarda, kurumsal kaynaklarda, veri tabanlarında ve bilgisayar programlarında bulunur (Small, 2005: 13). Elektronik posta, kurum kaynakları, dış kaynaklar, veri depoları, uzman kişiler gibi kaynaklar aracılığıyla açık bilgi kurum içerisinde paylaşılabilir (Smith, 2001: 315).

Alan yazın incelendiğinde açık ve örtük bilginin avantaj ve dezavantajlarının olduğu görülmektedir. Tablo 1'de Rooney, Hearn ve Ninan (2005: 197) Handbook On The Knowledge Economy isimli kitabından faydalanılarak açık ve örtük bilginin avantaj ve dezavantajlarından bahsedilmiştir.

Tablo 1. Açık ve Örtük Bilginin Avantaj ve Dezavantajları

Örtük Bilgi	**Açık Bilgi**
Avantajlar	
Başlangıçta görece kolay ve ucuzdur.	Bilgi teknolojileri tarafından herhangi bir zamanda herhangi bir yere anında taşınabilir.
Çalışanlar bilginin güvenilir olmasından olumlu etkilenebilir.	Kodlanmış bilgi, belirli bilgi biçimlerini kullanabilen kişilere proaktif olarak yayılabilir.
İleri bilgi yönetimi süreçlerinde ilgi uyandırması muhtemeldir.	Açıkça ifade edilen bilgiler tartışılabilir, danışılabilir ve geliştirilebilir.
Örtülü biçimde tutulan önemli bilgilerin rakiplere "sızma" olasılığı daha düşük olabilir.	Bilgiyi açık hale getirmek, organizasyondaki bilgi eksikliklerinin keşfedilmesini mümkün kılar.
Dezavantajlar	
Bireyler sahip olduklarını iddia ettikleri bilgiye sahip olmayabilirler.	İnsanların bilgilerini ifade etmelerine yardımcı olmak için önemli ölçüde zaman ve çaba gerekebilir.
Bireylerin bilgi profillerinin sık sık güncellenmesi gerekir.	Bilginin arttırılmasını motive etmek için kilit bilgi çalışanları ile istihdam ilişkisinin yeniden tanımlanması gerekebilir.
İnsanları hareket ettirmekle sınırlı olan bilgiyi transfer etme yeteneği, maliyetli ve organizasyon içinde bilginin yayılmasına erişimi ve hızı sınırlar.	Açık bilgi varlıklarını değerlendirmek için uzman komiteleri oluşturulmalıdır.
Kilit kişiler ayrılırsa, kuruluş önemli bilgilerini kaybedebilir.	Bir organizasyonda açık bilginin uygulanması, en iyi uygulamaların benimsenmesiyle sağlanmalıdır.

2.2. Bilgi Güvenliği

Bilginin iletilmeye, işlenmeye ve saklanmaya başlandığı andan itibaren bilginin korunması gerekmiştir (Dlamini, Eloff ve Eloff, 2008: 189). Bilgi teknolojisinin yaygın olarak benimsenmesi ve bilginin kuruluşlarda önemli bir varlık haline gelmesi (Xu, Wang ve Yan, 2021: 1), yeni ve karmaşık güvenlik açıklarını da beraberinde getirmektedir (Eloff ve Eloff, 2005: 10). Alan yazın incelendiğinde bilgi güvenliği tarihinin, bilgisayar güvenliği kavramıyla ilişkilendirildiği görülmektedir (Whitman ve Mattord, 2011: 4). Bilgisayar güvenliğine duyulan ihtiyaç, 2. Dünya Savaşı sırasında, ilk ana bilgisayarların geliştirildiği ve iletişim kodunun kırılmasına yönelik hesaplamalara yardımcı olmak için kullanıldığı zaman ortaya çıkmıştır (Whitman ve Mattord, 2011: 5). Bu dönemde en önemli güvenlik sorunu, bilgisayarlara kullanıcıları dışındaki kişilerin erişime açık olmamasını ve fiziksel bilgisayarın yabancılar tarafından çalınmamasını veya zarar görmemesini sağlamaktı (Dlamini vd. 2008: 190). Bu dönemde cihazları ve hizmet ettikleri görevleri korumak için çoklu güvenlik seviyeleri uygulanmaya başlamıştır (Whitman ve Mattord, 2011: 5). 1990'ların sonuna doğru saldırganlar solucan ve virüs kullanmaktan daha karmaşık saldırılara geçmiş, elektronik postalara veya web sitelerine kötü amaçlı kodlar yerleştirmeye başlamışlardır. Bu sorunların önüne geçmek için güvenlik duvarı uygulanmaya başlanmıştır ancak İnternet kullanımının yoğunlaşması güvenlik duvarının yeterli gelmemesine neden olmuştur. Bilgisayar korsanlığı topluluğu, ücretsiz olarak erişilebilen bilgisayar korsanlığı araçlarını ortaya çıkartmıştır. Bilişim teknolojilerinin tüm endüstrilerde yaygınlaşması, mobil cihazlarının ortaya çıkması ve artarak kullanılması ile 21. yüzyılda saldırılar da değişime uğramıştır. Artık saldırganlar finansal kazanç elde etmek için hackleme gibi farklı yöntemleri kullanmaya başlamışlardır (Dlamini vd., 2008: 192).

Bilişim teknolojilerinin gelişmeye devam etmesi yeni tehditlerin de ortaya çıkması ihtimalini doğurmaktadır. Bu nedenle fiziksel güvenlik, bilgi güvenliği farkındalığı, kimlik yönetimi ve çevre güvenliği gibi bilgi güvenliğinin sağlanmasına yönelik çalışmalara özen gösterilmesi gerekmektedir (Dlamini vd., 2008: 192).

2.2.1. Bilgi Güvenliği Prensipleri (Unsurları)

Alan yazın incelendiğinde bilgi güvenliğinin sağlanması için bilginin kullanılabilirlik, özgünlük ve gizlilik özelliklerinin korunması gerektiği vurgulanmaktadır (Vural, 2007: 40; Stamp, 2011: 2; Whitman ve Mattord, 2011: 14; Andress, 2014: 6). Bilginin her bir kritik özelliği başlıklar halinde incelenmiştir (Whitman ve Mattord, 2011: 14).

Gizlilik (Confidentiality): Gizlilik verilerin görüntülemeye yetkisi olmayan kişilerden koruma olarak tanımlanabilir (Stamp, 2011: 2; Andress, 2014: 6). Gizlilik, yalnızca bilgilere erişim hakları ve ayrıcalıklarına sahip kullanıcıların bunu yapabilmesini sağlamaktadır (Whitman ve Mattord, 2011: 15). Aynı zamanda elektronik ortamda bulunan veya taşınan bilginin yetkisiz ve izinsiz kişiler tarafından ele geçirilmesi durumunda bile anlamlı bir biçimde olmaması durumu da gizlilik olarak kabul edilmektedir (Vural, 2007: 40). Örneğin veri içeren bir dizüstü bilgisayarın kaybolması, biz bir şifre yazarken omzumuzun üzerinden bakan bir kişi, yanlış kişiye gönderilen bir e-posta eki, sosyal mühendislik, sistemlerimize giren bir saldırgan veya benzeri sorunlar gizliliği tehdit eden unsurlar arasında yer almaktadır (Andress, 2014: 6; Grama, 2020: 14).

Bilgilerin gizliliğini korumak için bazı önlemler alınabilir. Bilginin sınıflandırılması, şifreleme, erişim kontrolleri, güvenli belge saklama, güvenlik politikalarının uygulanması, bilgi

saklama görevlilerinin ve son kullanıcıların eğitimi bilgilerin gizliliğini korumak için alınacak önlemler arasında yer alabilir (Grama, 2020: 36; Whitman ve Mattord, 2011: 15). Gizlilik, bilginin çoğu özelliği gibi diğer özelliklerle birbirine bağlıdır ve mahremiyet olarak bilinen özellik ile yakından ilgilidir (Whitman ve Mattord, 2011: 15).

Bütünlük (Integrity): Bütünlük, verilerin yetkisiz veya istenmeyen bir şekilde değiştirilmesini önleme yeteneği olarak tanımlanabilir (Andress, 2014: 6). Bilgi tam, eksiksiz ve bozulmamış olduğunda bütünlüğe sahiptir (Whitman ve Mattord, 2011: 16). Verilerin tamamının veya bir kısmının yetkisiz olarak değiştirilmesi veya silinmesi; verilerin yetkili ancak istenmeyen bir şekilde değiştirilmesi veya silinmesi bütünlüğü tehdit eden durumlardır (Andress, 2014: 6; Grama, 2020: 37). Benzer bir ifadeyle bilginin bütünlüğü, bozulmaya, hasara, yok edilmeye veya özgün durumunun başka bir şekilde bozulmasına maruz kaldığında tehdit edilir. Aynı zamanda bilgi depolanırken veya iletilirken bozulma meydana gelebilir (Whitman ve Mattord, 2011: 16). Bütünlüğü korumak için yalnızca verilerde yetkisiz değişiklikleri önleyecek araçlara sahip olmak değil, aynı zamanda geri alınması gereken yetkili değişiklikleri tersine çevirme yeteneğine de ihtiyaç duyulmaktadır (Andress, 2014: 6). Güvenlik denetimleri, antivirüs yazılımları bilginin bütünlüğünün korunmasını sağlayabilir (Grama, 2020: 37).

Erişilebilirlik –Kullanılabilirlik (Availability): Erişilebilirlik en basit tanımıyla ihtiyaç duyulduğunda verilere erişme yeteneğini ifade etmektedir (Andress, 2014: 6). Kullanıcılar yetkileri dahilindeki bilgilere hızlı, güvenilir, zamanında ve güncel bir şekilde ulaşabilmeleri erişilebilirlik ile sağlanmaktadır (Vural, 2007: 41; Grama, 2020: 39).

Erişilebilirlik yetkili kullanıcıların (kişilerin veya bilgisayar sistemlerinin) herhangi bir müdahale veya engel olmaksızın bilgilere erişmesini ve gerekli formatta bilgileri almasını sağlamaktadır (Whitman ve Mattord, 2011: 14). Erişilebilirlik kaynaklı problemlerin çözümü için bilgi sistemlerinin bozulmalardan veya arızalardan hızlı bir şekilde kurtulması, birden fazla arıza noktasına sahip olunması, yedek ekipmanların bulunması gibi önlemler alınabilir (Grama, 2020: 39).

Orijinallik (Authenticity): Bilginin gerçekliği, bir çoğaltma veya fabrikasyondan ziyade, gerçek veya orijinal olma niteliği veya durumu olarak tanımlanabilir. Bilgiler, oluşturulduğu, yerleştirildiği, saklandığı veya aktarıldığı durumla aynı durumda olduğunda orijinaldir (Whitman ve Mattord, 2011: 15). Andress (2014: 8) ise orijinalliği, verilerin sahibi veya yaratıcısının bilinmesi olarak tanımlamaktadır ve orijinalliğin, dijital imzaların kullanılmasıyla güçlendirilebileceğini belirtmektedir (Andress, 2014: 8). Bu durum, bir kişinin e-posta göndermek gibi bir eylemde bulunmasını ve daha sonra bunu yaptığını reddetmesini engeller (Andress, 2014: 8).

Yarar (Utility): Fayda, verilerin bizim için ne kadar yararlı olduğu şeklinde tanımlanabilir (Andress, 2014: 9). Bilginin faydası, bir amaç veya amaç için değere sahip olma niteliği veya durumudur. Başka bir deyişle, bilgi bir amaca hizmet edebildiği zaman değerlidir. Bilgi mevcutsa ancak kullanıcı için anlamlı bir formatta değilse, yararlı değildir (Whitman ve Mattord, 2011: 17).

2.2.2. Kurumsal Bilgi Güvenliği

Güvenlik tehditleri arttıkça, kurumsal verileri koruma ihtiyacı kurumlar için hayati bir önem kazanmıştır (Galvez ve Guzman, 2009: 1). Kurumsal bilgi güvenliğinin amacı, bir kuruluşun bilgi, donanım ve yazılım gibi bilgi varlıklarını ve altyapısını yanlışlıkla veya kötü niyetli ifşa, değişiklik, silme ve kötüye kullanımından korumaktır (Gregory, 2003: 29; Peltier, 2013: 13). Kurumsal bilgi

güvenliği sadece teknolojik bir sorun değil aynı zamanda süreç ve iş yönetimi sorunu olarak kabul edilmelidir (Özcan, 2009: 47). Uygun önlemlerin seçilmesi ve uygulanması yoluyla kurumsal bilgi güvenliği, bir kuruluşun fiziksel ve finansal kaynaklarını, itibarını, yasal konumunu, çalışanlarını, diğer maddi ve maddi olmayan varlıklarını koruyarak iş hedeflerini veya misyonunu karşılamasına yardımcı olmaktadır (Peltier, 2013: 13). Kurumsal bilgi güvenliğinin sağlanması, örgüte rekabet avantajı, müşteri memnuniyeti, olumlu kurumsal imaj, güvenirlik, itibar gibi avantajlar sağlayabilir (Chang ve Ho, 2006: 348). Bilgi güvenliği ihlalleri maddi zarar, kurumsal sorumluluk ve güvenirlik kaybı gibi ciddi sonuçlar doğurabilir (Cavusoglu, Cavusoglu ve Raghunathan, 2004: 65) Risk yönetimi süreci uygulayarak kurumun karşı karşıya olduğu risklerin varlığı belirlenmeli, kurumun riskleri belirlendikten sonra kurumun misyonu ve hedeflerini karşılayacak uygun bilgi güvenliği yöntemleri belirlenmelidir (Peltier, 2013: 13). Kurumsal bilgi güvenliği bazı unsurlara dayanmalıdır (Peltier, 2013: 13):

- Bilgi güvenliği, kurumun hedeflerini veya misyonunu desteklemelidir.
- Bilgi güvenliği, güvene dayalı görevin ayrılmaz bir unsurudur.
- Bilgi güvenliği uygun maliyetli olmalıdır.
- Çalışanların ve yöneticilerin bilgi güvenliği sorumlulukları ve hesap verme sorumlulukları açıkça belirtilmelidir.
- Bilgi güvenliği, kapsamlı ve entegre bir yaklaşım gerektirir. Etkili bir bilgi güvenliği süreci için bilgi güvenliği konularının sistem geliştirme yaşam döngüsünün bir parçası olması gerekmektedir.
- Bilgi güvenliği periyodik olarak yeniden değerlendirilmelidir. Her şeyde olduğu gibi zaman ihtiyaçları ve hedefleri değiştirir. İyi bir bilgi güvenliği programı, düzenli olarak incelenmeli ve gereken her yerde ve zamanda değişikliklere açık olmalıdır.
- Bilgi güvenliği örgütün kültürüne uygun olmalıdır.

Üniversiteler bilgi açısından zengin örgütler olmaları nedeniyle sıklıkla bilgi güvenliği riskleri ile karşılaşabilmektedir (Yerby ve Floyd, 2018: 2). Yetkisiz not değişiklikleri, kişisel bilgilerin ele geçirilmesi, finansal ve kurumsal bilgi kaynaklarına erişim üniversitelerin sıklıkla karşılaştıkları bilgi güvenliği riskleri arasında yer almaktadır (Yerby ve Floyd, 2018: 3; Rezgui ve Marks, 2008: 241). Üniversitelerin bilgi varlıklarının riske atılmaması için bilgi güvenliği önlemlerinin alınması gerekmektedir (Rezgui ve Marks, 2008: 241).

2.2.2.1.Kurumsal Bilgi Güvenliği Tehditleri ve Güvenlik Açıkları

Güvenlik tehdidi, bir kişinin veya kuruluşun ağlarına, bilgisayarlarına, yazılımlarına veya verilerine zarar verme veya zarar verme yönünde kasıtlı eylemlerdir. Bilgi işleme sistemleri, çeşitli hasar türlerine neden olabilecek ve önemli kayıplarla sonuçlanabilecek birçok tehditle karşı karşıya kalabilir (Peltier, 2013: 16). Alan yazın incelendiğinde bilgi güvenliğine yönelik doğal afetler, teknik arızalar, prosedür eksikleri, zararlı yazılımlar, insan faktörü gibi birçok tehdidin bulunduğu belirlenmiştir (Gregory, 2003: 11; Muharremoğlu, 2013: 8; Peltier, 2013: 16). Güvenlik tehditleri kurum içinden veya kurum dışından gelebilir (Gregory, 2003: 11; Jouini, Rabai ve Aissa, 2014: 491). Kurum içinden veya kurum dışından kaynaklanan güvenlik tehditleri, insan, çevresel tehditler ve teknolojik tehditler olarak sınıflandırılabilir (Jouini vd., 2014: 493).

İyi veya kötü niyetli insan davranışları güvenlik tehdidi oluşturabilir. Çalışanların yanlışlıkla dosya silmesi veya kuruluşa zarar vermeyi amaçlayan saldırganlar insan tehdidi olarak

değerlendirilebilir (Grama, 2020: 42). Bilgi güvenliği tehditlerinden biri de saldırganlardır (Muharremoğlu, 2013: 8). Saldırganlar organizasyon için çok çeşitli faaliyetler ve etkiler içeren çok geniş bir tehdit kategorisidir. Hackerlar kuruluşun bilgi veya bilgi altyapısını bozmak, ifşa etmek veya zarar vermek amacıyla bir kuruluşun ağlarına ve sunucularına erişmek için kişisel olarak sahip olunan bilgisayarları kullanan bireyler veya gruplardır (Gregory, 2003: 12). Bilgileri çalıp daha sonra İnternet web sitelerine gönderebilir, rakiplere satabilir veya kimlik hırsızlığı yapmak için kullanabilirler. Aynı zamanda bilgisayar korsanları, bilgi güvenliği ihlallerinin oluşması için sosyal mühendislik eylemleri de gerçekleştirebilirler (Gregory, 2003: 17).

Doğal afetler, kazalar bilgi güvenliğini tehdit eden çevresel faktörler olarak değerlendirilebilir (Muharremoğlu, 2013: 8). Bu tür tehditler öngörülebilir değildir ve kuruluşlar bu tehditleri kontrol edemezler (Grama, 2020: 46). Çevresel tehditler, insan dışı etkenlerin neden olduğu tehditlerdir (Jouini vd., 2014: 494).

Bilgi güvenliği hedeflerine zarar vermek için bilgi sistemleri içinde işleyen tehditler teknolojik tehdit olarak değerlendirilmektedir (Grama, 2020: 46; Williams, 2008: 209). Virüsler, truva atları ve solucanlar, casus yazılımlar gibi kod veya kötü amaçlı yazılımlar; donanım ve yazılım arızaları, doğru çalışmayan süreçler teknolojik tehditler arasında yer almaktadır (Grama, 2020: 46; Gregory, 2003: 12). Teknolojik tehditler, bilgisayar donanım veya yazılıma yönelik sabotaj, özel veya kişisel olarak hassas bilgilerin çalınması ve ifşa edilmesi, bilgi altyapısına saldırılar, yaygın hasara neden olması amaçlanan bir virüs veya solucanın geliştirilmesi ve dağıtılması şeklinde gerçekleşebilir (Gregory, 2003: 11). Aynı zamanda malzeme üzerindeki fiziksel ve kimyasal işlemler de teknolojik tehditler olarak sınıflandırılmaktadır (Jouini vd., 2014: 494).

Alan yazın incelendiğinde bilgi güvenliği tehditlerinin birçok çeşidinin olduğu görülmektedir. Bu noktada karşımıza güvenlik açığı kavramı çıkmaktadır. Güvenlik açığı bilgisayar veya ağ donanımındaki veya yazılımın saldırıya veya hasara açık olmasını sağlayan donanım, yazılım veya süreçlerdeki herhangi bir zayıflık veya kusur olarak tanımlanabilir (Grama, 2020: 45; Gregory, 2003: 17; Williams, 2008: 208). Bir sistemdeki saldırganlar tarafından istismar edilebilecek ve tehlikeli etkilere yol açabilecek zayıflıklardan oluşan güvenlik açıkları (Jouini vd., 2014: 492), kasıtlı veya dikkatsizlik sonucu meydana gelebilir (Gregory, 2003: 24). Yapım ve tasarım hataları da güvenlik açığı olarak değerlendirilmektedir ve güvenlik açıkları teknoloji, süreç ve insan kaynaklı olabilir (Grama, 2020: 45). Yazılım hataları, işlevsel hatalardan, bir saldırganın uygulamaya veya tüm sistemi ele geçirmesine ve saldırmasına izin veren güvenlik açıklarına kadar, neredeyse sonsuz çeşitlilikte istenmeyen sonuçlar doğurabilir (Gregory, 2003: 24).

2.2.3. Kişisel Bilgi Güvenliği: Güvenlik Tehdidi ve Açığı İnsan

Bilgiye erişim ve bunları işleyen ortamların dinamik olması nedeniyle, sistem ve güvenlik gereksinimleriyle ilgili riskler sürekli değişime uğramaktadır (Peltier, 2013: 16). Artan harcamalar, alınan önlemlere rağmen kuruluşlar personel hataları nedeniyle bir dizi güvenlik olayıyla karşılaşmaktadır. Bilgi güvenliğine yönelik en büyük tehditlerden biri kuruluşların bilgi güvenliği politika ve prosedürlerine uymayan dikkatsiz çalışanlardan kaynaklanmaktadır (Siponen vd., 2010: 64; Diesch, Pfaff ve Krcmar, 2020: 1). Kurum çalışanlarının bilinçli veya bilinçsiz yaptıkları ihmaller, hatalar, dikkatsizlikler teknik anlamda alınan önlemlerin boşa çıkmasına neden olabilir (Özcan, 2009: 47). Kuruluşların çoğunlukla dış tehditlere karşı savunmasız olduğu genel algısının aksine, kötüye kullanım olaylarının çoğu aslında çalışanlar tarafından gerçekleştirilir (Chan vd.,

2005: 18). İnsanların bilgi güvenliği konusunda zayıf farkındalıkları veya farkındalıklarının olmaması bilgi güvenliği ihlallerinin ortaya çıkmasına neden olmaktadır (Chan vd., 2005: 19; Han, Dai, Han ve Dai, 2015: 2). Hem yönetimde hem de teknolojide çeşitli bilgi güvenliği önlemleri alınmasına rağmen fiili etkililik öncelikle insanların bilgi güvenliği konusundaki farkındalığına ve potansiyel risklerin farkında olmasına bağlıdır (Han vd. 2015: 2). Alan yazın incelendiğinde bilgi güvenliğini tehdit eden kişi odaklı faaliyetler olduğu görülmektedir. Örneğin sosyal mühendislik büyük ölçüde insan etkileşimine dayanmaktadır. Bu teknik bir saldırıdan ziyade diğer insanları güvenlik kurallarını çiğnemeleri ve hassas bilgileri paylaşmaları için kandırmayı içermektedir. Sosyal mühendislik saldırganları nezaket, yardımseverlik ve güven gibi insan doğasından yararlanmaktadır. Sosyal mühendislikte saldırganın nihai amacı, bilgisayar sistemlerine erişmek veya korunan alanlara erişmek için yeterli bilgiyi elde etmektir (Grama, 2020: 35).

Benzer şekilde kuruluş tarafından işini yürütmek için işe alınan, kurumun bilgi varlıklarına ve altyapısına erişebilen çalışanlar, kuruluşların kendilerine yüklediği güvene ihanet edebilir ve özel bilgileri dışarıdan birine ifşa edebilirler. Örneğin, çalışanlar rakip firmalara ticari sırları satabilir, organizasyonla ilgili hassas bilgileri basına sızdırabilir veya şirketin finansal bilgilerini paylaşabilir (Gregory, 2003: 12). Ayrıca ofiste bilgi kaynaklarının veya bilgisayar sistemlerinin açık bırakılması bilgi güvenliği ihlallerine neden olabilir. Çalışanların bu tür davranışları, kişisel çıkar sağlama veya kurumsal bilgi güvenlik sistemlerine zarar vermek için yapılan bilinçli davranışlardan ziyade dikkatsizlikten kaynaklanmaktadır (Chu ve So, 2020: 3).

Kurumsal kullanıcı hesabı yönetimi süreçlerindeki zayıflıklar, kullanıcı kimliklerinde tutarsızlıklara, çalışanlar kuruluştan ayrıldığında silinmeyen kullanıcı hesaplarına, çok fazla ayrıcalığa sahip kullanıcı hesaplarına ve etkili kullanıcı hesabı yönetimini ve kullanıcı hesabı incelemelerini engelleyen yetersiz veya zayıf kayıt tutma sonucunda gerçekleşebilir (Gregory, 2003: 24).

Kurum bilgilerin korunması söz konusu olduğunda kuruluşun karşılaştığı en büyük sorunlardan biri çalışanların bilgi, beceri ve bağlılık eksikliğidir (Thomson, Von Solms ve Louw, 2006: 7). Bir kuruluş içindeki kurumsal bilgi güvenliği kültürünün iyileştirilmesinin, politika ve prosedürlerle uyumluluğu iyileştirmesi gerektiğini ve daha sonra bir kuruluşun insan temelli risklerini azaltmaya yardımcı olması gerekmektedir (Parsons vd., 2015: 127). Bu noktada çalışanların eğitilmesi önem kazanmaktadır. Kurumun düzenleyeceği veya çalışanların katılacağı bilgi güvenliği eğitimi, öğretimi ve farkındalık faaliyetleri kurumsal bir bilgi güvenliğini teşvik eder aynı zamanda çalışanlarının bilgi güvenliği performansında artış sağlar (Peltier, 2013: 11). Eğitim, öğretim ve farkındalık faaliyetleri teknik olmayan en önemli önlemler arasında yer almaktadır (Colwill, 2009: 194).

2.2.4. Bilgi Güvenliği Politikaları

Bilgi güvenliği politikaları, kurumsal varlıkların nasıl korunması gerektiğini tanımlayan resmi ifadelerdir (Gregory, 2003: 76) ve kurum içinde bilgi güvenliğine yön veren belgelerdir (Höne ve Eloff, 2002: 402).

Bilgi güvenliği politikaları, çalışanların kuruluşlarındaki güvenlik politikalarından haberdar olmalarını ve onların kural ve yönergelerini takip etmelerini sağlamada önemli bir rol oynamaktadır (Kim ve Han, 2019: 860). Bir kuruluşun bilgi güvenliğini sağlama stratejisinin hayati bir parçası (Höne ve Eloff, 2002: 402) olan bilgi güvenliği politikasının rolü, bilgi varlıklarını korumak için "ne yapılacağını" tanımlamaktır (Gregory, 2003: 76). Temelde, bilgi güvenliği politikası,

kuruluşun tüm bilgi kaynağı kullanıcılarına bilgi güvenliği ihtiyacını ve kavramlarını açıklamak için hazırlanmaktadır (Höne ve Eloff, 2002: 402). Bu çalışanların bilgi sistemlerini doğru kullanmaya yatkın hale getirmeyi aynı zamanda içerden kaynaklanan tehditleri önlemeyi hedeflemektedir (Kim ve Han, 2019: 860). Gerçekleştirilen araştırmalar, bilgi güvenliği politikaları farkındalığının, bilgi güvenliğini koruma davranışları üzerinde olumlu etkiye sahip olduğunu göstermektedir (Li vd., 2019: 19).

Alan yazın incelendiğinde bilgi güvenliği politikasının aşağıdaki maddeleri içermesi beklenir (Fulford ve Doherty, 2003: 113; Gregory, 2003: 76; Khadraoui ve Francine, 2007: 263):

- Güvenlik ihtiyaçlarının belirlenmesi ve uygulanacak güvenlik önlemlerinin seçilmesi için risk analizi yapılmasını öneren ISO 17799 standartlarına uygun hazırlanmalıdır.
- Risk yönetimine ve esas olarak risk analizine dayalı metodolojik yaklaşımlar kullanılmalıdır.
- Bilgi sistemi ile ilgili yasal riskler dikkate alınmalıdır.
- Kuruluşun fiziksel bilgi varlıklarını ve bu varlıklara fiziksel erişimi korumak için alınan önlemleri içermelidir.
- Kuruluşun politikası virüs kontrol yazılımının uygulanması, eklerin kullanımı ve bilgi paylaşımı ile ilgili net olmalıdır.
- Gerekli koruma seviyelerini belirleyen bir sınıflandırma modeli de dahil olmak üzere korunacak bilgi varlıkları tanımlanmalıdır.
- Güvenlik politikası bilgilerin ifşası veya kullanımına ilişkin tüm kısıtlamaları vurgulamalıdır.
- Kullanıcıların bilgilere erişme ve işlevleri gerçekleştirme yetkisini tanımlamalıdır.
- Personelin sorumlulukları net bir şekilde açıklanmalıdır.
- Bilgilerin kullanılabilirliğini, gizliliğini ve bütünlüğünü sağlamak için alınacak önlemleri ele almalıdır.
- Kuruluşun bilgileri şifreleme / koruma gereksinimlerini ele almalıdır.
- Altyapı ve bilgi kaynaklarının korunmasına yönelik stratejileri ifade etmesi gerekir.
- Bir ihlal veya ihlalden kurtulmak için atılması gereken adımları ve bu tür güvenlik olaylarının kaydedilmesi için gereksinimleri belirtmelidir.
- İş gereksinimleri doğrultusunda erişim kontrollerinin nasıl tahsis edileceği ve yönetileceği konusunda açık bir rehberlik sağlamalıdır.
- Kuruluşun güvenli mobil bilgi işlemle ilgili duruşu ve uygulamaları vurgulanmalıdır.
- Güvenlik politikası, doğal afet gibi olaylara karşın acil durum planlarının nasıl yazılacağını, test edileceğini, sürdürüleceğini ve nihayetinde uygulanacağını belirtmelidir.
- İnternetin kurumsal kullanımı hızla artmaya devam ederken, politikanın özellikle pornografinin izlenmesi ve kişisel göz atma gibi konularla ilgili olarak İnternet erişimine yönelik kuralların açıkça belirlenmiş olması önemlidir.
- Tüm yeni sistemlere etkili güvenlik kontrollerinin yerleştirilmesini sağlamak için kılavuzlar sunmalıdır.
- Güvenlik değerlendirmelerinin tanımı ve nasıl gerçekleştirileceği ele alınmalıdır.

2.3. Örgütsel İletişim

Örgüt, belirli bir amaca ulaşmaya çalışan, işbirliğine dayalı faaliyetlerde bulunan iki veya daha fazla kişiden oluşan bir sistemdir (Barnard, 1968: 9). Miller (2008: 3415) ise örgütü, sosyal bir bütünlüğün varlığı, örgütsel ve bireysel hedefler, düzenli faaliyetler, örgütsel yapı, bir dış çevre ile bağlantı olmak üzere beş kritik özelliğe sahip yapı şeklinde tanımlamaktadır. Örgütler, otorite ilişkileri, iletişim sistemleri ve teşviklerin kullanımını içeren sınırlı yapılandırılmış sosyal etkileşim sistemleridir ve genellikle hiyerarşik bir yapıya sahiptirler (Champoux, 2010: 6). İnsanların örgütlenmeyi seçmelerinin birincil nedeni, birden fazla kişinin bilgi ve yetenekleriyle ortak bir amaca ulaşmaktır (Canary ve Mcphee, 2010: 7). Örgütün oluşturulması, personel işe alma, örgütün ürün ve hizmetlerini oluşturma ve geliştirme sürecinde; örgüt üyeleri birbirleri, müşteriler, tedarikçiler gibi paydaşlarla iletişim halindedir (Keyton, 2017: 506). Örgütleri anlama şekli üzerinde olumlu ve önemli bir etkiye sahip olan iletişim (Contractor ve Eisenberg, 1990: 151, Giri ve Kumar, 2010: 137), her türlü organizasyonun temel niteliklerinden biri olarak kabul edilmektedir (DeSanctis ve Monge, 1999: 694). Örgüt içerisindeki etkili iletişim yalnızca yöneticiler ve çalışanlar arasında uygun iletişim kanalları meydana getirmekten ziyade, aynı zamanda kurumun genel performansına dolaylı olarak katkıda bulunmak için de gereklidir (Yıldırım, 2014: 1100). Günümüzde giderek daha fazla çalışan ve işveren işlerinin önemli bir kısmının iletişim olduğunu fark etmektedir (Baker, 2007: 2; Giri ve Kumar, 2010: 137).

İletişim, bir mesajın göndericiden alıcıya çeşitli iletişim araçları aracılığı ile gönderilmesi olarak tanımlanabilir (Champoux, 2010: 322). İletişim sürecinin anahtar parçaları gönderici, kodlama, mesaj, kanal, kod çözme, alıcı, gürültü ve geri bildirim şeklindedir. Gönderici bir düşünceyi kodlayarak mesajı başlatır. Mesaj konuşma, yazma, jestler, mimikler şeklinde olabilir. Kanal ise mesajın içinden geçtiği ortamdır, resmi veya gayri resmi kanallar olabilir. Alıcı, mesajın yönlendirildiği kişi veya kişilerdir ve öncelikle sembolleri anlaşılır bir şekle çevirmesi gerekir. Bu adım mesajın kodunun çözülmesi adımı olarak kabul edilmektedir. Gürültü, algısal sorunlar, aşırı bilgi yüklemesi, anlamsal zorluklar veya kültürel farklılıklar gibi mesajın netliğini bozan iletişim engelleridir. Geri bildirim ise mesajın başlangıçta amaçlandığı gibi aktarmada ne kadar başarılı olduğunun kontrolüdür ve mesajın anlaşılıp anlaşılmadığının göstergesidir (Robbins ve Judge, 2013: 372).

İletişim ile ilgili alan yazın incelendiğinde iletişimin temel işlevinin bilgilendirme, yönlendirme, düzenleme, sosyalleştirme ve ikna etme yoluyla alıcı bilgisini veya davranışını etkilemek olduğu söylenebilir (Baker, 2007: 10). Örgütün arka planında iletişim, bilgiyi örgütteki daha geniş bir insan grubuna aktardığı için örgütsel başarı, canlılık ve uyum kaynağı için önemli bir faktör haline gelmektedir (Haroon ve Malik, 2018: 141). Bu noktada karşımıza örgütsel iletişim kavramı çıkmaktadır. Örgütsel iletişim, bireyler, gruplar veya ekipler gibi birkaç farklı türde gönderici ve alıcıdan veya bir bütün olarak organizasyonda çok çeşitli iletişim faaliyetlerini kapsamaktadır (Keyton, 2017: 506). Ayrıca örgütsel iletişim, örgütsel üyelerin örgütü yarattığı, sürdürdüğü ve değiştirdiği karmaşık ve sürekli bir süreçtir (Keyton, 2010: 13). Örgütsel iletişim çalışmaları ilk yıllarından itibaren hem sosyoloji, psikoloji, antropoloji ve hatta fizik bilimlerinden teorik çerçevelerden hem de örgütsel ortamlarda çalışanlardan etkilenmiştir (Miller, 2008: 3415).

Tüm iletişim biçimlerinin üç ana örgütsel hedefi bulunmaktadır. Örgütsel iletişimin birinci amacı, iş hedeflerine ulaşmak için çalışanların katılımını sağlamak ve arttırmaktır. İkinci olarak, çalışanların üretkenliğini arttırmak için iletişim sürecinin tüm katılımcılar arasında işbirlikçi çabaları geliştirmeyi hedeflemektedir. Üçüncü amaç ise psikolojik engelleri yıkarak örgüt

içerisindeki güven ortamını oluşturmaya yardımcı olmaktır. Örgüt içerisindeki engeller azaldıkça çalışanlar arasında daha yakın bağlar oluşmakta ve bu durum çalışanların başarısına katkıda bulunmaktadır (Ross, 2021: 305).

Örgütsel iletişim, ister kar amaçlı ister kar amacı gütmeyen, iş veya akademik tabanlı olsun, her tür kuruluşun işleyişi ve başarısında önemli bir unsur olarak görülmektedir (Baker, 2007: 10; Marques, 2010: 56). Ayrıca örgütsel iletişim, bir kuruluşun üyelerinin sağlığı ve kuruluşun dışarıdaki kişilerle olan ilişkisi için de önemlidir (Borca ve Baesu, 2014: 497). Uyum kazandırma, liderlik, çatışma yönetimi, anlam yaratma, motive etme ve etkileme, çatışmaların en aza indirilmesi, problem çözme ve karar verme, müzakere, pazarlık, işbirliğinin teşvik edilmesi, rehberlik sağlama, profesyonel ilişki kurulması, örgütün kurallarının uygulanması ve düzenlenmesi, örgütsel iletişimin temel işlevleri arasında yer almaktadır (Neher, 1997: 55; Gochhayat, Giri ve Suar, 2017: 694). Örgütsel iletişim, liderlerin çalışanlarına ulaşmasına ve onları organizasyonun vizyon, misyon ve hedeflerine ulaşmaları için motive etmelerine yardımcı olmaktadır (Gochhayat vd., 2017: 695).

Örgütsel iletişim, formel veya informel; planlı veya plansız, sözlü, sözsüz, yazılı veya görsel şekilde aynı zamanda yüz yüze veya dolaylı biçimde olabilir (Keyton, 2017: 506). Örgüt içerisinde üç tür iletişim süreci bulunmaktadır ve her iletişim türü farklı iletişim kanallarını içermektedir. Tek yönlü iletişim süreci, yalnızca göndericiden alıcıya hareket eden tek yönlü bir iletişim sürecini temsil etmektedir. Diğer bir iletişim süreci türü iki yönlü iletişimdir; hem gönderici hem de alıcı, bir iletişim kanalı kullanarak bilgi paylaşımı veya bilgi alışverişinde bulunmaktadır. Gönderici ve alıcı arasındaki kanal seçimi değişebilir. Üçüncü tür iletişim süreci ise çok boyutlu bir iletişim sürecidir. Çok boyutlu bir süreçte, iletişim sürecine dahil olan üç veya daha fazla katılımcı bulunmaktadır. Katılımcılar, göndericiler ve alıcılar şeklinde olabilir ve katılımcılar çeşitli iletişim kanallarını kullanabilirler (Ross, 2021: 306).

Örgüt içerisinde iletilen mesajlar birçok farklı biçimde olabilir ve farklı iletişim kanalları kullanılarak iletilebilir. Mesajlar, sözlü veya sözsüz, yazılı veya elektronik ortamlarda iletilebilir, bireye veya gruba yönelik olabilir. Bazı mesajlar ise sadece örgüt içerisinde çalışanlara iletilirken bazı mesajlar örgüt dışındaki kişilere iletilebilir (Keyton, 2010: 15). İletişim teknolojilerinde yaşanan büyük değişiklik örgütsel iletişim kanallarını da değişime uğratmıştır (Baker, 2007: 1). Örgüt içerisinde e-posta, sosyal medya, yönetici ve personel toplantıları ve konferans görüşmeleri dahil olmak üzere birden çok kanal kullanılarak iletişim sağlanabilir (Murphy, 2017: 21). Bu noktada kullanılacak kanalın seçilmesinin önemi ortaya çıkmaktadır. Örgütsel iletişimde kanal seçiminde beş temel özelliğe dikkat edilmesi gerekmektedir. İletişim kanalının güvenilirliği önemlidir. Bir kanalın güvenilirliği, kanalın tutarlı bir temelde çalıştığı ve kullanımının güvenli olması olarak tanımlanabilir. İletişim kanalı seçiminde bir diğer kriter de teslimat hızıdır. Gönderici veya alıcının bir mesajı hızlı bir şekilde göndermesi gerekiyorsa, kanal seçimi buna göre değişime uğramaktadır. Göndericinin veya alıcının dikkate alması gereken başka bir kriter ise iletişim kanalının etkinliğidir. Etkin bir iletişim kanalı ile iletişim sayesinde ulaşılmak istenen hedeflere ulaşma olasılığı artabilir veya azalabilir. İletişim sürecindeki katılımcı sayısı kullanılacak iletişim kanalının erişiminden etkilenmektedir. Örneğin toplu iletişim süreçleri için video konferans, e-posta, haber bültenleri ve yazılı raporlar kullanılabilir. Son olarak bir mesajın/fikrin karmaşıklığı, iletişim kanalı seçimini belirler. Mesajın karmaşıklığı farklı veya birden fazla iletişim kanallarının kullanılmasını gerektirebilir (Ross, 2021: 306).

Örgütsel iletişim seviyesi, formel ve informel, dikey, yatay, çapraz ile iç ve dış odak olarak ayrım yapılarak incelenebilir. Örgüt içerisindeki iletişim seviyeleri, kişilerarası iletişim, grup

düzeyinde iletişim, kurumsal düzeyde iletişim, kurumlar arası iletişim ve kitle iletişim biçiminde gerçekleşebilir (Baker, 2007: 4).

İletişim dikey, yatay veya çapraz olarak da karakterize edilebilir. Aşağı ve yukarı doğru iletişim akışlarını içeren dikey iletişim, hiyerarşik olarak konumlanmış kişiler arasında gerçekleşir (Baker, 2007: 4). Aşağı doğru iletişim, bir grubun veya organizasyonun bir seviyesinden daha düşük bir seviyeye akan iletişimdir (Robbins ve Judge, 2013: 373). Vizyon beyanı, stratejik hedefler, izlenecek stratejiler, operasyonel rehberlik konuları, politika geliştirme, politika uygulama konuları ve performans gibi konuları aktarılmaktadır (Ross, 2021: 313). Yukarı doğru iletişim ise grup veya organizasyonda daha yüksek bir seviyeye akar. Üst düzey kişilere geri bildirim sağlamak, hedeflere doğru ilerleme konusunda onları bilgilendirmek ve mevcut sorunları iletmek için kullanılır (Robbins ve Judge, 2013: 373).

Birbirleriyle hiyerarşik bir ilişki içinde olmayan kişiler arasındaki iletişim olan (Baker, 2007: 7) yatay iletişim, aynı çalışma grubunun üyeleri, aynı düzeydeki çalışma gruplarının üyeleri, aynı düzeydeki yöneticiler veya yatay olarak eşdeğer diğer çalışanlar arasında gerçekleşmektedir (Robbins ve Judge, 2013: 373). Farklı fonksiyonel bölümlerde bulunan yöneticiler ve çalışanlar arasındaki iletişim çapraz iletişim olarak ifade edilmektedir (Wilson, 1992).

Alan yazın incelendiğinde örgütsel iletişimi engelleyen veya geciktiren bazı bariyerlerin olduğu belirlenmiştir. Fiziksel engeller, coğrafi mesafe, sesler, kesintili İnternet bağlantısı, kapalı kapılar gibi iletişim sürecini kesintiye uğratan veya engelleyen somut şeylerdir. Örgüt içerisindeki çalışanların kullandıkları teknik dil, jargon gibi anlamsal engeller de iletişimin önündeki bariyerler olarak ortaya çıkmaktadır. Süreç engelleri ise gönderici ve alıcı arasındaki iletişim sürecinin herhangi bir noktada kesintiye uğramasıdır. Gönderici veya alıcı veya her ikisinin iletişim sürecini engelleyen psikososyal engeller olabilir. Gönderici/alıcı arasındaki psikolojik mesafe, zayıf dinleme becerisi psikososyal engeller arasında yer almaktadır. İletişim engellerinden bir diğeri de kültürel engellerdir. Farklı kültür biçiminde yetişen bireyler arasında iletişim engelleri yaşanabilir (Ross, 2021: 309).

Ayrıca iletişim becerileri eksikliği, kapalı iletişim ortamı, örgütsel yapı, yönetim ve çalışanlar arasında güven eksikliği, çalışanlar arasındaki rekabet, ego, filtreleme, algıda seçicilik, bilgi bombardımanı, duygular iletişim engelleri arasında yer almaktadır (Guffey ve Loewy, 2021: 22; Robbins ve Judge, 2013: 373). İlgili literatür incelendiğinde örgütsel iletişimin, örgütsel vatandaşlık (Yıldırım, 2014: 1100), örgüt kültürü, örgütün etkinliği (Gochhayat vd., 2017: 697), örgütsel performans (Haroon ve Malik, 2018: 147), iş tatmini ve iş performansı (Giri ve Kumar, 2010: 140), çalışanların motivasyonu (Rajhans, 2012: 83) ile ilgili olduğu belirlenmiştir.

Diğer örgütlerde olduğu gibi örgütsel iletişim karmaşık yapıya sahip olan üniversiteler içinde hayati bir rol oynamaktadır (Gizir ve Simsek, 2005: 197). Aynı zamanda üniversitelerde formel ve informel iletişim, çalışanların motivasyonunu ve performansını etkileyen değişkenler arasında yer almaktadır (Uslu ve Welch, 2016: 573).

2.3.1. Formel ve İnformel İletişim

Örgüt içerisindeki bireyler veya gruplar formel ve informel iletişim kurabilirler (Daniel ve Eze, 2016: 37; Kraut vd. 1990: 3). Formel iletişim, notlar, raporlar, kitaplar, prosedürler, web siteleri, dokümanlar gibi resmi ve planlanmış iletişim şeklidir. Ayrıca formel iletişim, kalıcılıkları ve kontrol edilebilmeleri nedeniyle yönetimsel perspektifleri temsil etmektedir (Keyton, 2010: 13). Formel iletişim önceden planlanmış, gündemi önceden belirlenmiş ve tek yönlüdür. Aynı zamanda

katılımcılar ve katılımcıların rolleri önceden belirlenmiştir, resmi dil kullanılmakta ve konuşmalar kayda alınabilmektedir (Kraut vd, 1990: 5). Kurumun resmi çalışmasına ilişkin mesaj alışverişini ifade etmektedir (Lunenburg, 2010: 1). Mesaj alışverişinde günlük konuşma dili yerine resmi ifadeler tercih edilebilir. Aynı zamanda formel iletişimde, yöneticileri diğer çalışanlardan ayırmak için unvanlar (müdür, sekreter veya yönetici asistanı gibi) kullanılabilir (Miller, 2011: 31).

Genellikle kişiler arası yatay iletişimle ilişkilendirilen informel iletişim, başlangıçta örgütsel performans açısından engel olarak görülmesine rağmen modern organizasyonlarda işin etkin bir şekilde yürütülmesini sağlamak için giderek daha önemli hale gelmiştir (Keyton, 2010: 91). İnformel iletişim planlanmamıştır, rastgele katılımcılardan oluşmaktadır, düzenlenmemiş gündem bulunmaktadır, etkileşimlidir, gayri resmi dil kullanılabilmektedir (Kraut vd.,1990: 5). Örgütsel sınırları aşan (Fish, Kraut, Root ve Rice, 1992: 37) informel iletişimin örgüt içerisinde ilişkisel ve kişisel faydaları bulunmaktadır. Ortak çalışma, gelecekte kişilerarası faaliyetler, kişilere yönelik olumlu algı, ortak payda geliştirmek informel iletişimin ilişkisel faydaları olarak belirtilirken; kişisel çıkarlar, bilgi edinme, işbirliği fırsatları informel iletişimin kişisel faydaları olarak belirtilmektedir (Zhao ve Rosson, 2009: 244).

Örgüt içerisindeki iletişimin büyük bir kısmı formel ve informel iletişim arasında sürekliliktedir ve çalışanlar arasındaki her etkileşim açıkça formel veya informel iletişim olarak kategorize edilemeyebilir (Koch ve Denner, 2022). Her iki iletişim biçimi örgüt yapısına katkıda bulunmaktadır (Shochley -Zalabak, 20156: 33).

2.4. Örgütsel Bilgi Paylaşımı

Yaşanan gelişmeler, bilginin sadece hızlı bir şekilde oluşturulmasını değil aynı zamanda bilginin hızlı edinilmesini ve uygulanmasını gerektirmektedir. Bunu gerçekleştirmenin en olası yöntemlerinden biri de bilgiyi etkili bir şekilde paylaşmaktır (Cheng, Ho ve Lau, 2009: 313). Bir işletmenin bilgiyi yaratma ve kullanma becerisine katkıda bulunan bilgi paylaşımı (Small, 2005: 2), en basit tanımıyla bir grup insan içinde bilgi alışverişi yapmaktır (Cheng vd., 2009: 314). Benzer bir tanımla bilgi paylaşımı, çalışanların bilgi, deneyim ve becerilerini tüm bölüm veya örgüt aracılığıyla alışverişini içeren sosyal etkileşim kültürü olarak tanımlanabilir (Zawawi vd., 2011: 60). Bartol ve Srivastava (2002: 65) ise bilgi paylaşımını, kurumsal olarak ilgili bilgileri, fikirleri, önerileri ve uzmanlığı birbirleriyle paylaşan bireyler şeklinde tanımlamaktadır. Bilgi paylaşımı, bilginin bireysel, grup, işletme ve işletmeler arası düzeylerde yayılmasıyla yakından ilgilidir (Small, 2005: 2). Bilgi paylaşımı sadece veri ve bilgi toplamaktan fazlasını içermektedir, bilginin değeri paylaşıldığında genişlemektedir (Cheng vd. 2009: 314). Bilginin paylaşılması, kişilerin bilgiyi elinde tutmasını değil, aynı zamanda değişim süreci aracılığıyla bilgiyi güçlendirmesine ve genişletmesine de olanak tanır. Örgüt içinde bilginin paylaşımı, organizasyonu gelecekteki gelişme ve büyümeye yönlendirmek için know-what ve know-how uygulamalarını tartışma fırsatı doğurmaktadır (Mitchell, 2005: 635). Bilgi paylaşımı bireysel veya örgütsel seviyede gerçekleşebilir (Zawawi vd., 2011: 60).

Bilgi paylaşımının amacı, bir bütün olarak örgütün iş hedeflerine ulaşmasına (Gurteen, 1999: 3), performansların iyileştirilmesine (Zawawi vd., 2011: 60), karar verme ve problem çözme süreçlerini geliştirmeye (Rahman, Mannan, Hossain, Zaman, ve Hassan, 2018: 762) yardımcı olmaktadır. Örgüt içerinde bilgi paylaşımı, bilgi yaratmayı, örgütsel öğrenmeyi ve performans başarısını etkileyen kritik bir süreç olarak değerlendirilmektedir (Bartol ve Srivastava, 2002: 73). Yeni bilginin yaratılması ve uygulanması, neredeyse tüm işletmelerin hayatta kalması için çok

önemlidir. Gurteen (1999: 2) bilgi paylaşımının kurumlar için neden önemli olduğunu beş başlıkta sıralamıştır:

- Fikirler, süreçler, bilgiler gibi somut olmayan ürünlerin payı küresel yapıda somut ürünlere göre giderek artmaktadır.
- Yenilik ve yeni bilgininin uygulanması sürdürülebilir rekabet avantajı sağlamaktadır.
- Personelin iş değiştirme ihtimalinin artması; bu durumda çalışanlardan biri organizasyondan ayrıldığında, bilgileri onlarla birlikte gidebilmektedir. Bilgi paylaşımıyla örgütte sadece o kişinin bilgiye sahip olmasının önüne geçilmektedir.
- Örgütte çalışanların birbirinin ne bildiği hakkında bilgi sahibi olmaması; örgütün bir bölümünde öğrenilen ve uygulanan uzmanlığın, başka bir bölümde kullanılmamasına yol açabilir.
- Teknoloji, iş ve sosyal hayatın değişimini hızlandırmaktadır. İşler değiştikçe, bilgi miktarı da artmakta aynı zamanda bilgiler eskimektedir, bilgi paylaşımıyla bu durum engellenebilmektedir.

Bilgi paylaşımını, temelde örgütsel faktörler, bireysel faktörler ve teknik faktörler olmak üzere üç faktör etkilemektedir (Zawawi vd., 2011: 60). Alan yazın incelendiğinde, bilginin doğası (Akgün, vd., 2009: 187), bireylerin sahip oldukları avantajlarını veya güçlerini kaybetme korkuları (Yang ve Wu, 2008: 1128), fikirlerinin çalınacağı korkusu (Azudin, Ismail ve Taherali, 2009: 142), kişisel özellikler (Matzler, Renzl, Müller, Herting ve Mooradian, 2008: 309), çevresel faktörler (Cabrera, Collins ve Salgado, 2006: 259), sistem özellikleri (Cabrera vd., 2006: 259) örgüt içindeki bilgi paylaşımını etkileyen faktörler olarak görülmektedir. Bilgi paylaşımı üzerinde kişisel özelliklerin etkileri araştırılan bir çalışmada, uyumluluk, vicdanlılık ve açıklık özelliklerinin bilgi paylaşımını etkilediği belirlenmiştir (Matzler vd., 2008: 309). Benzer bir çalışmada öz yeterlilik, uyumluluk, dürüstlük, yeniliğe açıklık, örgütsel bağlılık, algılanan destek, içsel ve dışsal ödüller, iş özerkliği, sistemin algılanan kullanılabilirliği ve sistemin algılanan kalitesinin bilgi paylaşımını etkilediği belirtilmiştir (Cabrera vd., 2006: 259).

Kamu çalışanlarının temel kaygısının kar etme algısı olmaması nedeniyle kamu çalışanlarının bilgi paylaşımını etkileyen faktörler özel bir değerlendirme gerektirmektedir. Diğer örgütlerdeki bilgi paylaşımını etkileyen faktörlerin yanı sıra kamu çalışanlarının bilgi paylaşımını özveri, şefkat, kamu yararına bağlılık, kamu politikası oluşturmaya yönelik ilgi de etkilemektedir (Chen ve Hsieh, 2015: 824).

Bilgi paylaşımı, çeşitli psikolojik ve örgütsel faktörlerden etkilenen karmaşık bir davranıştır ve bu faktörlerin uygun şekilde yönetilmesi, örgüt içerisindeki bilgi akışını sağlamaktadır (Cabrera vd. 2006: 259). Bu bağlamda örgütlerde bilgi paylaşımı önündeki engelleri kaldırmak için Gurteen (1999: 3-4) bilgi paylaşım kültürünün oluşturulması gerektiğini önermektedir. Bilgi paylaşım kültürünün oluşturulması içinde bilgi paylaşımının ödüllendirilmesi, bilgi güçtür paradigması yerine bilgiyi paylaşmak güçtür paradigmasının benimsenmesi, çalışanların bilgi paylaşımının motive edilmesi, işbirliğinin teşvik edilmesi, bilgi paylaşımının bireyden başlaması gerekmektedir (Gurteen, 1999: 3-4). Matzler ve arkadaşları (2008: 309) bilgi paylaşımı önündeki engellerin kaldırılması için kişisel özelliklerin de dikkate alınmasını önermektedir. Bartol ve Srivastava (2002: 68-69) bilgi paylaşımının önündeki engelleri kaldırmak için ödül verilmesi gerektiğini vurguladığı çalışmada bilgi paylaşımı nedeniyle çalışana verilen ödülün örgütün bilgi kaynaklarına katkı sağlayacağını, ekipler seviyesinde bilgi paylaşımının teşvik edeceğini vurgulamışlardır.

Cabrera ve Cabrera (2005: 731) gerçekleştirdikleri çalışmada bilgi paylaşımını teşvik etmek için insan yönetimi uygulamalarını aşağıdaki maddeler halinde sıralamışlardır:

- Çalışanlar arasında işbirliğini, karşılıklı bağımlılığı ve işlevler arası etkileşimleri teşvik eden iş tasarımlarının geliştirilmesi,
- Kişi-örgüt uyumuna ve iletişim becerilerine göre çalışanların seçilmesi,
- Katılımcı öz yeterliliğini arttırma, ekip çalışması becerilerini geliştirme, bilgiyi ifade etme ve iletişim kurma kapasitesini geliştirmeye yönelik eğitim programlarının hazırlanması,
- Resmi uyum ve sosyalleşme programlarının yanı sıra daha gayri resmi uygulama toplulukları ve sosyal etkinliklerin düzenlenmesi,
- Bilgi paylaşım davranışlarını önemseyen gelişimsel performans değerlendirmelerinin yapılması,
- Etkili bilgi paylaşımını ödüllendiren ve içsel ödülleri vurgulayan teşvik programlarının bulunması,
- İletişim, eşitlikçilik, adalet ve bilgi paylaşımı için güçlü normlara sahip destek ile sürdürülen açık ve güvenilir bir kültür oluşturulmalı,
- Kurumsal kültüre uyacak ve mevcut sosyal ağları güçlendirecek şekilde tasarlanmış, dikkatle seçilmiş, kullanıcı dostu bilgi teknolojisi kullanılmalıdır.

Bilgi paylaşımında teknoloji önemli bir aracı faktördür (Cheng vd., 2009: 315). İyi uygulanırsa ve insanlar bilgi paylaşımında teknoloji kullanımı konusunda eğitilirse, ihtiyaç duyulan bilgi ve enformasyona hızlı ve etkili bir biçimde ulaşabilir (Gurteen, 1999: 4). Bilgi paylaşımı uygulamaları ve teknolojilerini başarıyla uygulayan örgütler, gelişmiş kurumsal performans ve gelişmiş rekabet gücüne ulaşabilmektedir (Small, 2005: 2).

Üniversiteler, bilgi geliştirme ve yönetme rolleri nedeniyle bilgi tabanlı kuruluşlar olarak kabul edilmektedir (Goh ve Sandhu, 2013). Bilginin üretildiği, dağıtıldığı ve uygulandığı aynı zamanda bilgiye dayalı bir kurum olan üniversiteler için bilgi paylaşımı konusu da aynı derecede önemlidir (Cheng vd., 2009: 314; Jahani, Ramayah ve Effendi, 2011: 88). Üniversitelerde bilgi paylaşımının en bariz örneği bilgi sahibi kıdemli akademik personelin öğrenme ve öğretme süreçlerini geliştirmek için genç akademisyenlerle bilgi ve uzmanlığını paylaşması bir norm ve kültür olarak benimsenmiştir (Goh ve Sandhu, 2013: 41). Bu nedenle üniversitelerde bilgi paylaşımının teşvik edilmesi ve yaygınlaşması önemli görülmektedir (Fullwood vd., 2019: 131).

2.4.1. Açık ve Örtük Bilgi Paylaşımı

Örgüt içerisinde bilgi paylaşımını etkileyen faktörler arasında bilginin doğası da yer almaktadır. Bilginin açık veya örtük biçimde olması örgüt içerisindeki bilgi paylaşımını etkilemektedir (Ipe, 2003: 343). Açık bilgi, başkalarına aktarılması kolay olduğu için nispeten daha ucuz olarak kabul edilir. Buna karşılık, örtük bilgi, doğrudan temas ve çalışan davranışlarının gözlemlenmesi ile ilgili olduğu ve diğer çalışanlardan bilgi edinmenin daha karmaşık yollarıyla ilgili olduğu için daha yüksek bir değer taşır. Bu nedenle, doğası gereği, örtük bilginin paylaşılması açık bilgiye göre daha zordur, bu da örtük bilgiyi paylaşmayı daha maliyetli hale getirmektedir (Hau, Kim, Lee ve Kim, 2013: 357; Roberts, 2000: 431). Örtük bilginin paylaşımı, örgüt içerisinde çalışanların etkileşimleri ile sınırlıdır. Bu etkileşim örgütsel çevre ve örgütün özellikleri ile yakından ilişkilidir (Hwang, 2020: 2). Örgüt içerisindeki sosyal ilişkiler, çalışanlar arasındaki örtük

bilgi paylaşımını kolaylaştıran en önemli faktörlerin başında gelmektedir (Yang ve Farn, 2009: 211). Aynı zamanda yüz yüze etkileşim, gözlem, taklit, uygulama, deneyimlerin paylaşılması örtük bilgi paylaşımı yolları arasında yer almaktadır (Athanassiou ve Nigh, 2000).

Chen ve arkadaşları (2011: 3), gerçekleştirdiği çalışmada, açık bilgi paylaşımını içsel ve dışsal motivasyonun güçlendirdiğini; örtük bilgi paylaşımını ise dışsal motivasyondan ziyade içsel motivasyonun güçlendirdiği sonucuna ulaşmıştır. Benzer bir çalışmada karşılık beklentisinin açık ve örtük bilgiyi paylaşımını etkilediğini ayrıca örtük bilgi paylaşımı üzerinde güvenin ve işbirliğinin de etkilediği sonucuna ulaşılmıştır. Aynı çalışmada örtük bilgi paylaşımının açık bilgi paylaşımını güçlü bir şekilde etkilediği belirlenmiştir (Santos, Oliveira ve Curado, 2021).

Alan yazın incelendiğinde açık bilgi paylaşımı üzerinde dışsal motivasyonun, karşılık beklentisinin, duygusal zekanın, örgüt kültürünün, performans değerlendirilmesini, sanal topluluk ödüllerinin etkisi olduğu belirlenmiştir (Chen vd., 2011: 3; Fischer, 2021: 14; Imron vd., 2021: 4193; Malik, 2021: 627; Santos, Oliveira, ve Curado, 2021). Örtük bilgi paylaşımı üzerinde ise içsel motivasyonun, güvenin, işbirliğinin, karşılık beklentisinin, duygusal zekanın, iş deneyiminin, örgüt kültürünün etkisi olduğu belirlenmiştir (Chen vd., 2011: 3; Imron vd., 2021: 4193; Malik, 2021: 627; Santos, Oliveira ve Curado, 2021; Wang, Yin, Ma ve Liao, 2021; Salameh ve Zamil, 2020: 2233). İlgili alan yazın incelendiğinde örgüt içerisinde örtük bilgi paylaşımını, örgüt kültürü, bireysel özellikler, bilgi paylaşım kültürü, liderlik yapısı, yönetim tarzı ve örgüt yapısı gibi faktörler etkilerken; açık bilgi paylaşımını, liderlik yapısı, yönetim tarzı, bilişim teknolojileri desteği gibi faktörler etkilemektedir (Oliveira ve Pinheiro, 2021: 1300-1301; Yao vd., 2020: 621).

2.5. Literatür

Bu başlık altında bilgi güvenliği farkındalığı, kurumsal bilgi güvenliği, örgütsel iletişim ve örgütsel bilgi paylaşımı ile ilgili yapılan çalışmalara yer verilmiştir.

2.5.1. Kişisel Bilgi Güvenliği Farkındalığı İle İlgili Çalışmalar

İlgili literatür incelendiğinde özel ve kamu kurumlarında çalışan personelin bilgi güvenliği farkındalık düzeyini inceleyen çalışmalara rastlanmıştır. Aslan Öztezcan (2017) Marmara Üniversitesi'nde görev yapan akademik ve idari personelin bilgi güvenliği farkındalığını incelediği çalışmada, katılımcıların bilgi güvenliği farkındalığının ortalamanın üzerinde olduğu sonucuna ulaşmıştır. Güldüren (2015), doktora tez çalışmasında üniversitelerde görev yapan akademik personele bilgi güvenliği farkındalığını kazandırmak için çoklu ortam materyallerinden oluşan bir web sitesi geliştirmiş ve bu web sitesinin etkililiğini incelemiştir. Araştırma sonucunda web sitesinin bilgi güvenliği farkındalığı kazandırmada etkili olduğu görülmüştür.

Özdemir (2019) kamu çalışanlarının bilgi güvenliği farkındalığını incelemiştir. Araştırma sonucunda kamu çalışanlarının bilgi güvenliği farkındalık düzeyinin orta seviyede olduğu, bilgi güvenliği eğitimi almış personelin bilgi güvenliği farkındalığının daha yüksek olduğu belirlenmiştir. Benzer bir çalışmada Alemdaroğlu (2020), bankacılık sektöründe çalışan personelin bilgi güvenliği farkındalığına ilişkin algılarını incelemişlerdir. Araştırma sonucunda erkek çalışanların daha fazla güvenlik önlemi aldığı, üst düzey yöneticilerin kişisel verilerin korunması ve bilgi güvenliği bilinci konularında daha hassas olduğu sonucuna ulaşılmıştır. Bilen (2016) gerçekleştirdiği yüksek lisans tez çalışmasında kamu kurumunda çalışan personelin bilgi güvenliği farkındalığını ve demografik bilgilere göre farklılaşmasını incelemiştir. Araştırma sonucunda kamu kurumunda çalışan teknik personelin bilgi güvenliğinin yeterli düzeyde olduğu, diğer personelin

ise yeterli düzeyde bilgi güvenliği farkındalığına sahip olmadığı belirlenmiştir. Kapanoğlu (2016), yüksek lisans tez çalışmasında öğretmenlerin bilgi güvenliği farkındalığını belirlemeye çalışmıştır. Farklı branşlardan 1355 öğretmen ile gerçekleştirdiği çalışmada öğretmelerin bilgi güvenliği farkındalığının orta düzey olduğu sonucuna ulaşılmıştır.

Puspitaningrum, Devani, Putri, Hidayanto ve Hapsari, (2018) bir devlet kurumunda çalışan üst düzey yöneticilerin bilgi güvenliği farkındalığını belirlemeye yönelik bir çalışma gerçekleştirmişlerdir. Çalışma sonucunda katılımcıların bilgi güvenliği seviyesinin orta düzey olduğunu belirtmişler. Araştırma sonucunda çalışanların bilgi güvenliği farkındalık düzeyini izlemek ve iyileştirmek için işletme, teknoloji ve insan açısından belirli stratejiler yapılması gerektiği önerisinde bulunmuşlardır. Çatuk (2018), gerçekleştirdiği doktora tez çalışmasında Kobilere yönelik bilgi güvenlik farkındalığı ölçeği geliştirmiştir.

Çelik Çöp (2017), yüksek lisans tez çalışmasında, kamu hastanelerinde görev yapan kalite yönetim direktörlerinin bilgi güvenliğini farkındalığını belirlemek amacıyla "Bilgi Güvenliği Farkındalık Ölçeği"ni uygulamışlardır. Araştırma sonucunda katılımcıların genel bilgi güvenliği farkındalık düzeyinin orta düzeyde olduğu ancak katılımcıların teknik konularda yeterli bilgiye sahip olmadığını belirlemiştir. Ender Akcan (2019), elektronik hasta kayıtlarının gizliliği ve güvenliğine ilişkin gerçekleştirdiği yüksek lisans tez çalışmasında özel sağlık sigorta şirketi çalışanlarına bilgi güvenliğine ilişkin soruların yer aldığı anketi uygulamıştır. Araştırma sonucunda çalışanların yarısından fazlasının bilgi güvenliği eğitimine katıldığı ve bilgi güvenliğine duyarlı olduğu sonucuna ulaşmıştır. Kurt (2019) gerçekleştirdiği çalışmada üniversite hastanesinde çalışan personelin bilgi güvenliği tutumlarını incelemiştir. Araştırma sonucunda erişim ve yetkilendirme, örgütsel güvenlik ve güvenlik politikaları algılarının iyi düzeyde olduğu, benimsenen güvenlik algılarının orta düzeyde olduğu belirlenmiştir. Başdinkçi (2017), yüksek lisans tez çalışmasında, sağlık kurumlarında farklı meslek gruplarında çalışan personelin bilgi güvenliği farkındalığını araştırmıştır. Araştırma sonucunda genel olarak katılımcıların bilgi güvenliği farkındalığına sahip olduğu ayrıca şifre paylaşılması, hasta bilgilerinin sızdırılması, veri güvenliğinin sağlanmaması, kötü niyetli kişiler, lisanssız yazılım kullanımı kurumlarındaki en önemli bilgi güvenliği risk faktörleri olarak değerlendirilmiştir. Taner (2018) yüksek lisans tez çalışmasında emniyet personelinin bilgi güvenliği farkındalık düzeyini tespit etmek amacıyla 404 jandarma ve polise bilgi güvenliği farkındalık ölçeğini uygulamıştır. Araştırma sonucunda katılımcıların bilgi güvenlik farkındalık düzeyinin ortalamanın altında olduğu belirlenmiştir. Mart (2012), bilişim kültüründe bilgi güvenliği farkındalığını incelediği çalışmada, farklı meslek gruplarından 501 kişiye bilişim kültüründe bilgi güvenliği farkındalığı anketini uygulamıştır. Araştırma sonucunda, bilişim kültürleri ve bilgi güvenliği farkındalığı arasında pozitif yönlü bir ilişki olduğu ayrıca teknoloji kullanımı ve bilgi güvenliği arasında da pozitif yönlü bir ilişki olduğu belirlenmiştir (Mart, 2012). Genç (2019), İnternet kullanıcılarının bilgi güvenliği farkındalığını, riskli davranışlar, korumacı davranışlar, suça maruz kalma ve tehlike algısı bağlamında incelemiştir. Araştırma sonucunda, riskli davranışlar ile korumacı davranışlar, suça maruz kalma arasında pozitif yönde anlamlı bir ilişki olduğu, riskli davranışlar ile tehlike algısının ilişkisiz olduğu belirlenmiştir.

Akyol (2013), COBIT iç denetim sisteminin kurulu olduğu özel bir sigorta şirketi çalışanlarına bilgi, eğilim, davranış, farkındalık durumlarını kapsayan bir bilgi güvenliği anketi uygulamıştır. Araştırma sonucunda çalışanların bilgi güvenliği ile bilgi, eğilim ve farkındalık sahibi olduğu ancak bunu davranışlarına yansıtma konusunda problem yaşadıkları belirlenmiştir. Kızılelma (2014) doktora tez çalışmasında, ISO 9000 kalite ve ISO 27000 bilgi güvenliğine yönelik

bir ölçek geliştirerek bir hastane çalışanlarına uygulamışlardır. Araştırma sonucunda, hasta güvenliği, kalite ve bilgi güvenliği faktörlerinin sağlık mükemmelliğini etkilediği görülmüştür.

Aloul (2012), çalışmasında Birleşik Arap Emirlikleri'nde yer alan üniversitelerde yapılan çalışmaları inceleyerek bazı okullar, üniversiteler, devlet kurumları ve özel kuruşlar için bilgi güvenliği farkındalığının oluşturulması amacıyla çeşitli önerilerde bulunmuşlardır. Bu öneriler, siber suç yasalarının oluşturulması ve uygulanması, acil müdahale ekiplerinin kurulması, işletmelerin çalışanlarına ve müşterilerine güvenlik eğitimi verilmesi, telekomünikasyon şirketlerinin İnternetin güvenli kullanılmasıyla ilgili çalışmalar yapması, okullar ve üniversitelerin güvenlik konularını bilgisayar derslerine entegre etmesi şeklindedir (Aloul, 2012).

Kişisel bilgi güvenliği ile ilgili alan yazında yer alan çalışmalar incelendiğinde, farklı meslek gruplarında görev yapan çalışanların bilgi güvenliği farkındalığının araştırıldığı, genellikle katılımcıların bilgi güvenliği farkındalığının orta düzey ve üzeri olduğu, bilgi güvenliği farkındalığını belirlemeye yönelik ölçme araçlarının geliştirildiği, bilişim kültürü ve teknoloji kullanımı ile bilgi güvenliği arasında pozitif yönlü ilişki olduğu belirlenmiştir.

2.5.2. Kurumsal Bilgi Güvenliği İle İlgili Çalışmalar

Alan yazın incelendiğinde kurumsal bilgi güvenliğini etkileyen veya kurumsal bilgi güvenliği ile ilişkili faktörlerin araştırıldığı çalışmalara rastlanmıştır.

Ünver (2019) 413 insan kaynakları çalışanı ve yöneticilerin bilgi güvenliği farkındalıklarını incelediği çalışmasında, katılımcıların bilgi güvenliği politikası bilincinin teorik anlamda var olmasına rağmen iş süreçleri yönetilirken bilgi güvenliği uygulamalarının göz önünde bulundurulmadığı belirlenmiştir.

François, (2016) kurumsal bilgi güvenliği programlarını etkileyen faktörleri incelediği doktora tez çalışmasında, bilgi güvenliği politikaları farkındalığı ile bu politikaları uygulamanın kurumsal bilgi güvenliğini olumlu etkilediği sonucuna ulaşmıştır. Benzer bir çalışmada Parsons ve arkadaşları (2015), bilgi güvenliği kültürü ile çalışanların bilgi güvenliği politika ve prosedürlerine ilişkin bilgileri ve tutumları, bireysel davranışları bağlamında bilgi güvenliği karar verme arasındaki ilişkileri incelemişlerdir. Araştırma sonucunda bilgi güvenliği kültürüne sahip kuruluşlarda çalışanların, bilgi güvenliği politika ve prosedürlerine uygun olarak bilgi, tutum ve davranışlara sahip olma durumuyla arasında pozitif yönlü bir ilişki olduğu belirlenmiştir. Parsons ve arkadaşları (2014), bilgi güvenliğinin insan kaynaklı açıklarını belirlemek için bir ölçek geliştirmişler ve bu ölçeği 500 çalışana uygulamışlardır. Araştırma sonucunda, kurumun bilgi güvenliği politika bilgisi ve tutumu, bilgi güvenliği davranışlarını açıkladığı ayrıca çalışanların politika ve prosedür bilgilerinin politika ve işleme yönelik tutumu kendi bildirdiği davranışlardan daha güçlü bir şekilde etkilediği belirlenmiştir.

Chan, Woon ve Kankanhalli (2005) lojistik ve kimya endüstrilerinde çalışan katılımcılarla gerçekleştirdikleri çalışmada kurum içerisindeki bilgi güvenliği politikalarına ve yönergelerine uyumlu davranış gösterilmesi ile çalışanların bilgi güvenliği öz yeterliliği, algılanan bilgi güvenliği iklimi ve çalışanların kurum içerisinde sosyalleşmesi arasında pozitif bir ilişki olduğu sonucuna ulaşmışlardır. Kraemer, Carayon ve Clem (2009) örgütsel ve insani faktörlerin bilgi güvenliğiyle arasındaki ilişkiyi incelediği çalışmada odak grup görüşmeleri yapmış ve ağ analizi tekniğini kullanmıştır. Araştırma sonucunda bilgi güvenliğini etkileyen faktörleri dış etkiler, insan hatası, yönetim, organizasyon, performans ve kaynak yönetimi, politika sorunları, teknoloji ve eğitim olarak tespit etmişlerdir. Furnell ve Rajendran (2012) bir örgütün çalışanlarının bilgi güvenliği

davranışlarını etkileyen muhtemel faktörleri anlamak ve ilişkilendirmek amacıyla bir model geliştirmiştir. Geliştirilen modelde, örgütsel faktörlerin, işyeri etkileşiminin, bilgi güvenliğiyle ilgili yaşanan olayların bilgi güvenliği davranışını yüksek derecede etkilediği belirlenmiştir.

Rezgui ve Marks (2008), yükseköğretimde görev yapan personelin bilgi güvenliğini etkileyen faktörleri incelediği çalışmada, kültürel yapı, inançlar, sosyal koşullar, personel davranışları, işe yönelik tutumların bilgi güvenliğini etkilediğini belirtmiştir. Mahabi (2010), gerçekleştirdiği doktora tezinde bir üniversitede yer alan sistem yöneticilerinin ve kullanıcılarının bilgi güvenliği uygulamaları ve kullanıcı bilincine ilişkin algılarını incelemiştir. Araştırma sonucunda kullanıcıların güvenlik saldırılarına karşı korunabilmeleri için kullanıcı bilinçlendirme eğitimine ihtiyaç duydukları belirlenmiştir ve bilgi güvenliği uygulamalarında insan faktörünün göz önünde bulundurulması gerektiği vurgulanmıştır. Demirok (2016), kurumsal bilgi güvenliği yönetim sistemini bir vakıf üniversitesi örneği üzerinden gerçekleştirmiştir. Kurumsal bilgi güvenliğinin sadece cihazlar ve politikalarla sağlanamayacağı nedeniyle insan faktörünü göz önüne alarak çeşitli eğitimler düzenlemiştir. Kurumsal bilgi güvenliğinin kurum kültürü olarak benimsenmesi gerektiği tespit edilmiştir. Hadlington ve arkadaşları (2019), 1003 çalışanla gerçekleştirdiği çalışmada, çalışma taahhüdünün, iş kimliğine bağlılığın ve iş kontrol odağının bilgi güvenliği ile arasındaki ilişkiyi incelemiştir. Araştırma sonucunda daha fazla dışsallık gösteren çalışanların bilgi güvenliğine daha az bağlı olduğu, iş kontrol odağının bilgi güvenliğini yordadığı belirlenmiştir. Stanton, Stam, Guzman ve Caledra (2003), gerçekleştirdiği çalışmada örgütsel bağlılığın bilgi güvenliği davranışına etkisini incelemişlerdir. Araştırma sonucunda örgütsel bağlılığı fazla olan çalışanların bilgi güvenliğini tehdit eden davranışlarını daha az gösterdiği belirlenmiştir. Lee (2015), algılanan özerkliğin, algılanan yetkinliğin ve algılanan ilişkinin çalışanların güvenlik politikası ile uyumlu davranışına etkisini araştırmıştır. Sonuçlar algılanan özerkliğin, algılanan yetkinliğin ve algılanan ilişkinin güvenlik politikasına uygun davranışı önemli ölçüde öngördüğünü göstermiştir. Aslandağ (2010) yüksek lisans tez çalışmasında bilgi güvenliği unsurları olan gizlilik, bütünlük ve kullanılabilirliğin, müşteri memnuniyetine, örgütsel bağlılığa, çalışan memnuniyetine ve süreç yaklaşımına etkisini incelemiştir. Araştırma sonucunda bilgi güvenliği unsurları ve müşteri memnuniyeti, örgütsel bağlılık, çalışan memnuniyeti ve süreç yaklaşımı arasında pozitif yönlü olumlu bir ilişki olduğu belirlenmiştir.

Tu ve arkadaşları (2018) gerçekleştirdikleri çalışmada bir organizasyondaki bilgi güvenliği yönetimini etkileyen ve başarısına katkıda bulunan etmenleri incelemişlerdir. Araştırmada 219 çalışanla gerçekleştirdikleri çalışma sonucunda, örgütsel farkındalık ve üst yönetim desteğinin bilgi güvenliği yönetimi başarısında en önemli katkıları sağladığı sonucuna ulaşmışlardır. Aktan (2017), doktora tez çalışmasında bir devlet üniversitesinde görev yapan akademik personelin örgüt kültürünün bilgi güvenliği algısına etkisini incelemiştir. Araştırma sonucunda örgüt kültürünün bilgi güvenliği algısını olumlu etkilediği, aynı zamanda örgüt kültürünün bilgi güvenliğinin gizlilik, bütünlük, erişilebilirlik, sorumluluk prensibi algısını da olumlu etkilediği belirlenmiştir. Gerçeker (2012), hastane yöneticileri ile gerçekleştirdiği çalışmada örgüt kültürü ve bilgi güvenliği yönetimi arasında pozitif güçlü bir ilişki olduğu sonucuna ulaşmıştır.

Aydoğmuş (2010), gerçekleştirdiği yüksek lisans tez çalışmasında sekiz farklı sektörden 80 farklı firmada çalışan bilgi güvenliği yöneticilerine ve sorumlularına ISO/IEC 17799: 2005 standardı esas alınarak bir anket uygulamıştır. Araştırma sonucunda kurumdaki bilgi güvenliği kurallarının ve kontrollerin yönetimin onayı ile gerçekleştirildiği belirlenmiştir. Tuygun (2019) yüksek lisans tez çalışmasında, kamu kurum personeliyle gerçekleştirdiği çalışmada ISO27001

Bilgi Güvenliği Yönetim standardının uygulanabilirliğini incelemiştir. Araştırma sonucunda ISO27001 sertifikasyon sürecini, yönetim kadrosunun ve teknik ekip üyelerinin bilgi güvenliğini sağlamada olumlu katkı sağladığını belirtirken; bilgi güvenliği yönetim sistemleri kadrosu ise teknik yeterlilik, eğitim gibi konularda takviyeye ihtiyaç duyduklarını belirtmişlerdir. Özhan (2019), yüksek lisans tez çalışmasında bilgi güvenliğinin kurumların itibarına etkisini incelemiştir. Araştırma sonucunda bilgi güvenliği mimarisinin kurumların itibarı üzerinde doğrudan etkisi olduğu, finansal kurumların itibarlarını korumak için bilgi güvenliğine önem vermeleri gerektiği vurgulanmıştır.

İlgili alan yazın incelendiğinde kurumsal bilgi güvenliğinin sağlanması için bazı önlemlerin alınması gerektiği çalışmalara rastlanmıştır.

Sauerwein ve arkadaşları (2019) gerçekleştirdikleri çalışmada kamu kurumlarında yer alan bilgi kaynaklarını bilgi türü, bütünleşme, zamanlılık, özgünlük, kaynak türü ve güvenilirlik alt boyutlarına dayalı olarak sınıflandırmışlardır. Çalışmada 68 kamu bilgi güvenliği veri kaynağı tanımlanmış ve sınıflandırılmıştır. Araştırma sonucunda bilgi güvenliği ve risk yönetimi süreçleri için entegrasyonunu ve kullanımını zorlaştıran çok çeşitli heterojen bilgi güvenliği veri kaynaklarının yer aldığı belirlenmiştir.

Vural (2007), gerçekleştirdiği yüksek lisans tez çalışmasında kurumsal bilgi güvenliği, bilgi güvenliğini tehdit eden unsurlar ve sızma testleriyle ilgili kapsamlı bir araştırma gerçekleştirmiştir. Araştırma sonucunda bilgi güvenliği yönetim sistemlerinin geliştirilmesi, örgütsel önlemlerin alınması tavsiye edilmektedir.

Singh ve Margam (2018), Delhi Merkez Üniversiteleri kütüphanelerinin bilgi güvenliği önlemlerini inceledikleri çalışmada kütüphanelerin güvenlik programlarına teknik önlemlerin yanı sıra bilgi güvenliği politikaları, güvenlik prosedürleri ve farkındalık yaratma etkinlikleri gerçekleştirmesi gerektiği vurgulanmıştır. Abdelwahed, Mahmoud ve Bdair (2016) Filistin'de yer alan üniversitelerde yönetim bilgi sistemini kullanan bilişim merkezi ve idari bölümde çalışan katılımcılarla bilgi güvenliği politikaları ile yönetim bilgi sistemlerinin etkinliği arasındaki ilişkiyi incelemişlerdir. Araştırma sonucunda bilgi güvenliği politikaları ile yönetim bilgi sistemlerinin etkinliği arasında pozitif yönde anlamlı bir ilişki olduğu sonucuna ulaşmışladır. Demirtaş (2013), yüksek lisans tez çalışmasında bilgi güvenliği yönetim sistemi belgesine sahip 24 firmaya bilgi güvenliği yönetim sisteminin başarı dayanaklarını ve gereklerini belirlemeye yönelik bir anket uygulamıştır. Çalışma sonucunda firmaların bilgi güvenliği yönetim sistemini kuruluşun imajını arttırmak, sahip olduğu bilgi kaynaklarını korumak, riskleri kontrol altında tutmak için kullandıkları belirlenmiştir. Aynı çalışmada bilgi güvenliği yönetim sisteminin, kuruluşun iş süreçlerine, teknoloji gelişimine ve insan kaynakları gelişimine olumlu katkı sağladığı belirlenmiştir. Alasulu (2012), bilgi güvenliği yönetim sistemi ve kalite yönetim sistemi arasındaki ilişki ile benzerliklerini incelemiş ve bir işletmede kalite yönetim sistemi ile bilgi güvenliği yönetim sistemi kurulumu yapılmıştır. Çalışma sonucunda kalite yönetim sistemi ile bilgi güvenliği yönetim sisteminin birbirini tamamladığı, sistemin etkinlik ve verimliliğini arttırdığı belirlenmiştir.

May ve Lane (2006) 38 Avustralya rektör yardımcısı ile üniversitelerin bilgi güvenliği yönetiminin mevcut durumunu, karşılaşılan sorunları ve geliştirmesine yönelik yapılacak çalışmalara yönelik bir araştırma gerçekleştirmişlerdir. Araştırma sonucunda bir model önerisinde bulunmuşlardır. Geliştirilen modelde, teknolojik önlemlerin alınmasının ve bilgi güvenliğinin örgütün kültürüne uyumlu olması gerektiği belirtilmiştir. Henkoğlu (2015) doktora tez çalışmasında, Avrupa Birliği güvenlik politikaları, Türk Hukuk Mevzuatında hassas bilgi

varlıklarına ilişkin düzenlemeleri ve 15 üniversitede bilgi güvenliği kapsamında kilit noktalarda çalışanların bilgi güvenliği önlemlerine ilişkin bulguları dikkate alarak üniversiteler için bilgi güvenliği politikası geliştirmiştir.

Vardal (2009), gerçekleştirdiği doktora tez çalışmasında, alan yazını inceleyerek bilgi güvenliği standartlarını belirleyerek yükseköğretim kurumları için insan ve bilgi merkezli bilgi güvenlik modeli önermiştir. Ayrıca geliştirilen modelin pilot uygulamaları yapılmış ve modeli kullanan katılımcılara anket uygulanmıştır. Araştırma sonucunda katılımcıların bilgi güvenliğinin önemi ve gerekliliği, bilgi güvenliğinin sağlanmaması durumunda çeşitli zararların ortaya çıkabileceği konusunda yüksek katılımın olduğu sonucuna ulaşmıştır. Benzer bir çalışmada Özcan (2009), bilgi güvenliğine zarar verebilen tehditler, kurumsal bilgi güvenliği standartları açıklanarak bilgi güvenliği yönetim sistemi detaylı bir biçimde tanıtılmıştır. Ayrıca araştırma sonucunda bilgi güvenliğinin yönetilmesinin sadece bilgi güvenliğini sağlamada yeterli olmayacağı; insan, eğitim ve teknoloji temelli yaklaşımların belirlenmesi gerektiği vurgulanmıştır (Özcan, 2009). Karimi (2018), doktora tez çalışmasında kurumlar için bilgi güvenliği, davranış, farkındalık, politika, yönetim ve kültür bileşenlerinin yer aldığı bir bilgi güvenliği çerçevesi oluşturmuştur. Geliştirilen çerçeve Türkiye, İran ve İsveç'te örgütlerde uygulanarak sonuçlar değerlendirilmiştir. Araştırma sonucunda, bilgi güvenliği eğitimi alan kişilerin bilgi güvenliği farkındalığının daha fazla olduğu, bilgi güvenliği politikalarının ve yönetimin bilgi güvenliği farkındalığını ve kültürünü olumlu etkilediği belirlenmiştir (Karimi, 2018).

Çek (2017) gerçekleştirdiği yüksek lisans tez çalışmasında bilgi güvenliği standartları ve bilgi güvenliğinde insan faktörüne odaklanmıştır. Araştırma sonucunda, bilgi güvenliği kurumda çalışan her bir çalışanın bilgi güvenliği süreçlerine dahil edilmesi gerektiği, bilgi güvenliğinin iş sürecinin bir parçası olduğu vurgulanmıştır. Gülmüş (2010), kurumsal bilgi güvenliğini tehdit eden riskler, ülkemiz bilişim mevzuatı ve hukuku incelenerek kurumların bilgi varlıklarını korumak için alınabilecek önlemleri belirtmiştir. Araştırma sonucunda, bilgi güvenliği öneminin kamu kurumlarında tam olarak kavranmadığı, çalışanların sebebiyet verdiği kazaların en az saldırılar kadar kurumları tehdit ettiği, kişilerin görev ve sorumluluklarının kılavuzlarla tanımlanması gerektiği belirtilmiştir.

Yıldız (2007), yüksek lisans tez çalışmasında, bilgi teknolojileri yönetimi standartlarından ISO 20000 ve COBIT standartları incelemiş, bilgi teknolojileri açısından kurumların var olan durumu araştırılmış, bilgi güvenliği bağlamında kurumlara hareket planı önermiştir. Gencer (2015), bilgi güvenliğinin kanun ve yönetmeliklerdeki yeri, ISO 27001 bilgi güvenliği standardı incelenmiş ve kurumsal bilgi güvenliğinin sağlanması amacıyla bilgi güvenliği kontrol yazılımı geliştirmiştir. Ayrıca kurumsal bilgi güvenliğinin sağlanması için çalışanlara bilgi güvenliği ile ilgili bilgilendirme toplantıları gerçekleştirilmiştir. Kahraman (2006), TS ISO/IEC 27001/17799 standartlarına göre bilgi güvenliği yönetim sistemi gerekleri ve bu gerekler ışığında ASELSAN firmasının bilgi güvenliği yönetim sistemine uygulama biçimini incelemiştir. Ergen (2007), BS 7799 / ISO 17799 standardına dayalı bir bilgi güvenliği yönetimi çerçevesi önermiş ve bu çerçeveyi bir devlet üniversitesindeki seçilen iki kuruluşa uygulamıştır. Çetinkaya (2008), gerçekleştirdiği yüksek lisans tez çalışmasında kurumların bilgi güvenliği tedbirlerini uygulama başarısını belirlemek amacıyla web tabanlı bir test aracı geliştirmiştir ve geliştirilen test aracı 22 firmada kullanılmıştır. Ayrıca kamu veya özel kurumlar için bilgi güvenliği yönetişim modeli geliştirilen (Tok, 2010), bilgi güvenliği yönetimi standardının kurulumu ve yönetilmesine yönelik kılavuz

hazırlanan (Mete, 2010; Ganbat, 2013; Gürsel, 2019) bilgi güvenliği çerçevesi oluşturulan (Sarıkoz, 2015) birçok çalışma yer almaktadır.

Bilgi güvenliğinin teknik konularına yönelik çalışmalar incelendiğinde, bilgi güvenliğini tehdit eden saldırılara yönelik saldırı tespit sistemleri (Canlı, 2009; Altun, 2014), bilgi güvenliği ihlallerini engellemek için yazılımı geliştirilmesi (Koç, 2017), bilgi güvenliğini tehdit eden unsurların teknik nedenler (Muharremoğlu, 2013), bilgi güvenliği risk analizi yazılımı (Şahinaslan, 2010; Eminağaoğlu, 2011; Beken, 2019), bilgi güvenliği yönetim sistemi otomasyonu/ yazılımı (Bingöl, 2010; Gemci, 2010; Kocamustafaoğulları, 2013; Altınpulluk, 2016) içerikli tezlere de rastlanmıştır.

Kurumsal bilgi güvenliğine yönelik ilgili literatürde yer alan çalışmalar incelendiğinde, bilgi güvenliği politikalarına yönelik bilgi ve farkındalığın, kültürel yapı, örgütsel yapı eğitim, teknoloji, sosyal koşullar, çalışan davranışları gibi değişkenlerin bilgi güvenliğini etkilediği belirlenmiştir.

2.5.3. Örgütsel İletişim İle İlgili Çalışmalar

İlgili literatür incelendiğinde özel ve/veya kamuda çalışan personelin örgütsel iletişim düzeyi, örgütsel iletişimi etkileyen faktörleri araştıran çalışmalara rastlanmıştır.

Ölçer ve Koçer (2015), üniversitelerde görev yapan akademik personelin örgütsel iletişim düzeyini incelemişlerdir. Araştırma sonucunda akademik personelin iletişiminin yeterli düzeyde olmasına rağmen bilimsel bilgi paylaşımının yetersiz düzeyde olduğu, akademisyenlerin motivasyon eksikliği yaşadığı sonucuna ulaşılmıştır. Katırcı (2021), gerçekleştirdiği yüksek lisans tez çalışmasında üniversitelerde görev yapan X ve Y kuşağı idari personelin örgütsel iletişim değerlerini incelemiştir. Araştırma sonucunda, kuşaklar arasında örgütsel iletişim yönünde farklılığın olmadığı sonucuna ulaşılmıştır.

Blazenaite (2011), gerçekleştirdiği çalışmada etkili bir örgütsel iletişim için iletişim sistemi modeli geliştirmiştir. Araştırmada ilgili literatür incelenerek iletişim sistemini etkileyen iç (örgütsel kültür, örgütsel hedefler, yönetim felsefesi, liderlik tarzı, örgütsel yapı, bireysel yapı, ödül sistemi, örgütün sahip olduğu teknolojiler) ve dış (sosyal, politikal, teknolojik, kültürel unsurlar) unsurlar belirlenmiş, bu unsurlar göz önüne alınarak örgütsel, yönetimsel, grup ve kişilerarası seviyede iletişim için önerilerde bulunulmuştur (Blazenaite, 2011).

Gochhayat, Giri ve Suar (2017), teknik ve yönetim alanlarında görev yapan personelle gerçekleştirdikleri çalışmada, örgütsel kültür ile örgütsel iletişim arasında pozitif yönde anlamlı bir ilişki olduğu sonucuna ulaşmışlardır. Haroon ve Malik (2018) örgütsel iletişimin üniversitelerdeki örgütsel performansa etkilerini inceledikleri çalışmada, örgütsel iletişimin örgütsel performans üzerinde anlamlı bir etkisi olduğu belirlenmiştir. İnce ve Gül (2011), kamu kurumunda çalışan personelle gerçekleştirdikleri çalışmada örgütsel iletişim ve örgütsel adalet türleri arasında pozitif yönde bir ilişki olduğu sonucuna ulaşmışlardır. Çanak ve Avcı (2016), öğretmenlerin örgütsel iletişim ve örgütsel özdeşleşme düzeylerini araştırdıkları çalışmada, örgütsel iletişim ve örgütsel özdeşleşme arasında pozitif yönde bir ilişki olduğu sonucuna ulaşmışlardır. Topsakaloğlu (2015), yüksek lisans tez çalışmasında kamu kurumunda çalışan personelin örgütsel iletişim ve örgütsel bağlılık düzeyleri arasındaki ilişkiyi incelemişlerdir. Araştırma sonucunda örgütsel iletişim ve örgütsel bağlılık arasında pozitif yönde anlamlı bir ilişki olduğu sonucuna ulaşılmıştır.

İlgili literatür incelendiğinde formel ve informel iletişim biçimlerini inceleyen çalışmalara rastlanmıştır.

Daniel ve Eze (2016) özel şirket çalışanları ile gerçekleştirdikleri çalışmada formel ve informel iletişim ile örgüte duygusal bağlılık ve devam bağlılığı arasında pozitif yönde anlamlı bir ilişki olduğu belirlenmiştir. Polat, Lynn, Akgün ve Emre (2018) yeni ürün geliştiren farklı sektörde çalışan katılımcılarla gerçekleştirdikleri çalışmada, takım özerkliği, takım istikrarı, takım üyelerinin deneyimi, takım gücünün güven aracı değişkelerinin formel ve informel iletişimi etkilediği sonucuna ulaşmışlardır.

Örgütsel iletişim ile ilgili alan yazın incelendiğinde örgütsel kültür, örgütsel adalet, örgütsel özdeşleşme, örgütsel bağlılık, duygusal bağlılık ve örgütsel iletişim arasında pozitif yönlü bir ilişki olduğunu gösteren çalışmalara rastlanmıştır.

2.5.4. Örgütsel Bilgi Paylaşımı İle İlgili Çalışmalar

Alan yazın incelendiğinde örgüt içerisinde bilgi paylaşımını etkileyen çeşitli faktörler olduğu ve bu faktörleri belirlemeye yönelik çalışmaların yapıldığı belirlenmiştir. Malezya'da özel bir üniversitede çalışan akademisyenler arasındaki bilgi paylaşımını inceledikleri çalışmada Cheng vd. (2009), bilgi paylaşımını etkileyen faktörleri örgütsel, bireysel ve teknolojik faktörler olarak sınıflandırmışlardır. Araştırma sonucunda teşvik sistemlerinin ve kişisel beklentinin, akademisyenlerni bilgi paylaşım faaliyetine katılmaya iten iki temel faktör olduğu belirlenmiştir (Cheng vd., 2009). Fullwood ve Rowley (2017) gerçekleştirdikleri çalışmada üniversite görev yapan akademik personelin bilgi paylaşımını etkileyen faktörleri inceledikleri çalışmada, örgüt kültürünün, inançların, öznel normların bilgi paylaşma davranışlarını ve niyetlerini etkilediğini belirlemişlerdir.

Akademisyenlerin bilgi paylaşımını etkileyen bireysel ve örgütsel faktörleri nitel yöntemle inceleyen Fullwood, Rowley ve McLean (2019), karşılıklı güvenin, liderlik özelliklerinin, örgüt yapısının, teknolojinin, bireysel özelliklerin, düzenli yüz yüze iletişimin bilgi paylaşımını olumlu etkilediği sonucuna ulaşmışlardır. Chen ve Hsieh (2015) kamu personelinin bilgi paylaşımını etkileyen faktörleri inceledikleri çalışmada, özveri, şefkat, kamu yararına bağlılık, kamu politikalarını oluşturmaya yönelik ilginin bilgi paylaşımını etkileyen motivasyonlar arasında yer aldığını belirtmişlerdir. Benzer bir çalışmada kamu çalışanlarının etkili bilgi paylaşımını etkileyen faktörlerin açık liderlik iklimi, başarısızlıktan öğrenme, bilgi kalitesi, performans yönelimi, değişim sürecinden memnuniyet, değişim vizyonu olduğu belirlenmiştir. Bu özellikler örgüt iklimi, alt yapı ve süreçler, strateji uygulama genel başlıkları altında incelenmiştir (Taylor ve Wright, 2004: 28).

Melenli (2011) yüksek lisans tez çalışmasında kamu kurumunda çalışan personelin bilgi paylaşma davranışını etkileyen faktörleri incelemiştir. Araştırma sonucunda, etik ve iş tatminin bilgi paylaşımını olumlu etkilediği kişi-örgüt uyumunun ise olumsuz etkilediği belirlenmiştir.

İlgili literatür incelendiğinde bazı çalışmalarda bilgi paylaşımının daha iyi anlaşılabilmesi için örtük ve açık bilgi paylaşımı olarak araştırıldığı çalışmalara da rastlanmıştır. Hau vd. (2013), örtük ve açık bilgi paylaşımını etkileyen faktörleri incelediği çalışmada, örgütsel ödüllerin açık bilgiyi paylaşımını olumlu etkilerken örtük bilgi paylaşımını olumsuz etkilediği sonucuna ulaşmışlardır. Aynı çalışmada karşılıklılık, eğlence ve sosyal sermayenin, çalışanların örtük ve açık bilgi paylaşma niyetlerini arttırmaya önemli ölçüde katkıda bulunduğu belirlenmiştir (Hau vd., 2013). Rahman ve arkadaşları (2018), üniversitede görev yapan akademik personelin örtük bilgi paylaşımını etkileyen faktörleri incelemişlerdir. Araştırma sonucunda, dışadönüklük, uyumluluk, duygusal istikrar, açıklık, motivasyon, öz yeterlik, karşılıklı güven özelliklerinin örtük bilgi

paylaşımı üzerinde önemli bir rol oynadığını belirlemişlerdir. Allameh, Pool, Jaberi ve Soveini (2014), açık ve örtük bilgi paylaşımının kurum performansı üzerinde olumlu etkisi olduğu sonucuna ulaşmışlardır. Aslan (2014), işletmelerde açık ve örtük bilgi paylaşımı ve inovasyonun performansa etkisini inceledikleri çalışmada, bilgi paylaşımının inovasyon üzerinde etkisi olduğu sonucuna ulaşmıştır. Ayrıca bilgi paylaşımı ile firmanın finansal performansı arasında pozitif bir ilişkisi olduğu belirlenmiştir. Yeşil ve Mavi (2021), kamu hastanesinde görev yapan sağlık çalışanları ile gerçekleştirdikleri araştırmada örgütsel güvenin açık ve örtük bilgi paylaşımı üzerine etkisini incelemişlerdir. Araştırma sonucunda, yöneticiye güvenin açık ve örtük bilgi paylaşımını olumlu yönde etkilediği sonucuna ulaşmışlardır. Hwang (2020) özel şirket çalışanları ile gerçekleştirdiği çalışmada çalışanların çoğunun (%90) örtük bilgi edineceği kişinin rahat iletişim kurabilen biri olmasını tercih ettiği sonucuna ulaşmıştır. Akgül ve Yavuz (2021) örtük bilgi paylaşımının algılanan örgütsel destek ve çalışan yaratıcılığı üzerinde anlamlı ve pozitif etkisi olduğu sonucuna ulaşmışlardır.

Örgütsel bilgi paylaşımı ile ilgili alan yazın incelendiğinde örgüt yapısının, bireysel faktörlerin, teknolojik faktörlerin, kişisel beklentilerin, yüz yüze iletişimin bilgi paylaşımını etkilediğine yönelik çalışmalara rastlanmıştır. Ayrıca ilgili alan yazında açık bilgi paylaşımını, örgütsel ödüllerin, eğlence, sosyal sermaye ve örgütsel güven etkilerken örtük bilgi paylaşımını özyeterlik, sosyal sermaye, güven, motivasyon gibi değişkenler etkilemektedir.

Alan yazın incelendiğinde kurumsal bilgi güvenliği ile bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşma değişkenlerini ayrı ayrı inceleyen çalışmalara rastlanmıştır.

Gumus (2007), üniversitede çalışan personelle gerçekleştirdiği çalışmada bilgi paylaşımı ve iletişim tarzı, iletişim memnuniyeti arasında pozitif yönlü güçlü bir ilişki olduğu sonucuna ulaşmıştır.

Bulgurcu vd. (2010) gerçekleştirdiği çalışmada çalışanların genel bilgi güvenliği farkındalığının kurumsal bilgi güvenliği politikalarına uyma davranışını doğrudan ve dolaylı olarak etkilediği sonucuna ulaşmışlardır.

Baran (2019), yüksek lisans tez çalışmasında özel öğretimde görev yapan personelin örgütsel bilgi paylaşımına yönelik tutumları ve bilgi güvenliği arasındaki ilişkiyi araştırmıştır. Araştırma sonucunda örgütsel bilgi paylaşımı ve bilgi güvenliği arasında pozitif yönde anlamlı bir ilişki olduğu, aynı zamanda örgütsel bilgi paylaşımının bilgi güvenliği üzerinde anlamlı ve olumlu bir etkisinin olduğu belirlenmiştir. Aynı çalışmada bilgi güvenliğinin arttırılması için örgütsel bilgi paylaşımının teşvik edilmesi gerektiği vurgulamıştır.

Arhin ve Wiredu (2018) bilgi güvenliğini örgütsel iletişim bağlamında incelemiştir. Örgütsel iletişimin güvenlik ihlallerini önlemede etkili olduğu, çalışanlar arasındaki iletişimin desteklenmesi gerektiği belirlenmiştir. Safa ve Von Solms (2016) bilgi güvenliği bilgi paylaşımının bilgi güvenliği etkisini incelediği çalışmada, 482 çalışana bilgi paylaşımını etkileyen içsel ve dışsal motivasyon kaynakları ile ilgili maddelerin yer aldığı bir ölçek uygulamışlardır. Araştırma sonucunda içsel ve dışsal motivasyonun bilgi güvenliği bilgi paylaşımı üzerine olumlu etkisi olduğunu belirlemişlerdir.

Alan yazında, kurumsal bilgi güvenliğine yönelik çalışmalar incelendiğinde bilgi güvenliği yönetim sistemleri, bilgi güvenliği kontrol yazılımları, bilgi güvenliği farkındalığı, bilgi güvenliğini tehdit eden unsurlar, bilgi güvenliğini etkileyen örgütsel ve bireysel faktörlerin araştırıldığı çalışmalar yer almaktadır. Ancak kurumsal bilgi güvenliğinin örgütsel iletişim, örgütsel bilgi paylaşımı gibi boyutlarının da beraber incelendiği çalışmaların bulunmadığı belirlenmiştir ve tez konusu bu bağlamda ortaya çıkmıştır.

2.6. Bilgi Güvenliği, Örgütsel İletişim Ve Bilgi Paylaşım İlişkisi

Örgütler bilgi, veri, donanım, yazılım ve ağlar gibi birçok bilgi varlığına sahip olduğu bilgi ekonomisinde yaşamaktadır (Martins ve Eloff, 2002: 203). Elektronik ağlar ve bilgisayar tabanlı bilgi sistemlerindeki hızlı gelişmeler, çoğu kurumda veri işlemek, depolamak ve iletmek için kullanılarak örgütlere çeşitli yetenekler kazandırmaktadır (Dhillon ve Backhouse, 2000: 125). Örgütlerin devamlılığının sağlanması için bilginin üretilmesi ve paylaşılması büyük önem taşımaktadır (Baran, 2019: 3). Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler, kurumların bilgi varlıklarının öneminin giderek artmasını ve aynı zamanda kurumsal bilgi varlıklarının korunmasının önemini ortaya çıkartmıştır (Dhillon ve Backhouse, 2000: 125). Günümüzde bilgi güvenliği açıklarının maliyetli sonuçları bulunmaktadır (Kraemer vd., 2009: 510). Bilgi kaynaklarının örgüte sağladığı rekabet avantajı göz önünde bulundurulduğunda, örgütlerin yüksek düzeyde bilgi güvenliğini sağlama ve uygulama ihtiyacı artmaktadır (Parsons vd., 2015: 117). Ancak örgütler en iyi biçimde tasarlanan ve uygulanan güvenlik sistemlerine sahip olsalar bile güvenlik sistemleri insan davranışlarından etkilenmektedir (Furnell ve Rajendran, 2012: 12). Bilgi güvenliği açıkları incelenirken sadece teknolojik veya programlama hatası olmayacağı fark edilmeli, insan ve örgüt faktörlerinin etkisi olabileceği göz önünde bulundurulmalıdır (Kraemer vd., 2009: 509). Alan yazın incelendiğinde bilgi güvenliğini dış etkiler, insan hatası, yönetim, organizasyon, performans ve kaynak yönetimi, politika sorunları, teknoloji ve eğitim gibi faktörlerin etkilediği belirlenmiştir (Kraemer vd., 2009: 518). Yapılan çalışmalar kurumsal bilgi güvenliğinin araştırılırken bireysel bilgi güvenliği farkındalığının incelenmesi gerektiğini vurgulamaktadır (Parsons vd., 2015: 127). Ayrıca işin yapısı, yönetim, işyerindeki etkileşim gibi örgütsel faktörlerin kurumsal bilgi güvenliğini etkilediği çalışmalara rastlanmaktadır (Furnell ve Rajendran, 2012: 15). Örgüt içerisinde bilginin güvenliğinin sağlanmasında ve paylaşılmasında örgütün özellikleri etkili olmaktadır (Baran, 2019: 3).

Bilgi paylaşımı, üniversiteler dahil tüm örgütlerde bilgi yönetimi uygulamalarının başarısı için hayati öneme sahiptir. Çalışanların kuruluşun bilgi kaynaklarından yararlanabilmesi için etkin bir bilgi paylaşımı gerekmektedir (Cheng vd., 2009: 322). Güven, dürüstlük örgüt içerisinde bilgi paylaşımına olumlu katkı sunmaktadır (Sharratt ve Usoro, 2003: 190). Örgüt içerisindeki iletişim şeklinin bilgi paylaşımı üzerinde etkisi bulunmaktadır. Örgüt içerisinde bilgi paylaşımı, çalışanlar arasında formel iletişimle bilgi paylaşımı ve informel iletişimle bilgi paylaşımı şeklinde gerçekleşebilir (Boland ve Tenkasi, 1995: 364). Örgüt içerisindeki çalışanların günlük sosyal iletişim kurmaları, iş saati dışında görüşmeleri veya bir arada bulunmaları yani informel iletişim halinde olmaları aralarındaki iletişimi güçlendirerek bilgi paylaşımını arttırmaktadır (Azudin vd., 2009: 146). İşle ilgili deneyimleri tartışmak amacıyla yapılan düzenli toplantılar, işbirlikçi bir ortam oluşturan ve herkesin yararlandığı bir bilgi paylaşımı için bir yol sağlayabilir (Azudin vd., 2009: 146). Benzer bir çalışmada Azudin ve arkadaşları (2009: 157), Malezyada bir örgüt içerisinde çalışanlar arasındaki informel iletişimin bilgi paylaşımına etkisini incelemişlerdir. Araştırma sonucunda informel iletişim kuran kişilerin bilgi paylaşım düzeylerinin fazla olduğunu ve bu durumun bilgi paylaşımını olumlu etkilediği sonucuna ulaşmışlardır. Esnek, merkezi olmayan, informel iletişimin yaygın olduğu örgütler, örtük bilgi paylaşımını teşvik etmektedir (Sharratt ve Usoro, 2003: 188).

Çalışanların bilgi paylaşımını etkileyen örgütsel faktörler, bireysel faktörler ve teknik faktörler olmak üzere temelde üç faktör bulunmaktadır. Teknik faktörler, bilgi paylaşımında kullanılan yazılım ve donanımlar gibi bilgi yönetim teknolojileridir. Bireysel faktörler, inançlar,

algılar, beklentiler, tutumlar ve duygular gibi kişisel özelliklerdir. Örgütsel faktörler ise örgüt kültürü, yönetim anlayışı, örgütsel iletişim gibi örgüt yapısıyla ilişkili özellikler olarak ifade edilebilir (Cheng vd., 2009: 315).

Ticari amacı olmayan kamu kuruluşu çalışanlarının bilgi paylaşımını etkileyen faktörlerin incelenmesi gerektiği vurgulanmıştır (Chen ve Hsieh, 2015: 824). Benzer bir çalışmada, örgütlerde informel iletişimin bilgi paylaşma üzerine etkisinin incelenmesi gerektiğini belirtmişlerdir (Azudin vd., 2009: 159). Nie, Lin, Ma ve Nakamori, (2010: 249) ise örgüt içerisinde informel ve formel iletişimin, örtük ve açık bilgi paylaşımı ile aralarındaki ilişkilerin incelenmesine yönelik çalışmalar yapılması gerektiği vurgulanmıştır (Nie, Lin, Ma ve Nakamori, 2010: 249). Ancak formel ve informel iletişim ile örtük ve açık bilgi paylaşımı arasındaki ilişkinin incelendiği çalışmaya rastlanmamıştır. Bilgi güvenliği sadece ticari kaygısı olan kuruluşlar için değil tüm kuruluşlar için büyük önem taşımaktadır. Bu bağlamda yükseköğretim kurumları hem iç iş süreci hem de dış varlıkları açısından birçok değerli bilgiye sahiptir ve bilgi güvenliği yükseköğretim kurumları için önem arz etmektedir (Sari, 2012: 469).

3. YÖNTEM

Bu bölümde araştırma yöntemi ve modeline, evren ve örneklemine, veri toplama sürecine, veri toplama araçlarına ve veri analizine yönelik bilgiler sunulmuştur. Araştırma soruları, örneklem, veri toplama araçları ve analiz yöntemleri Tablo 2'de özetlenmiştir.

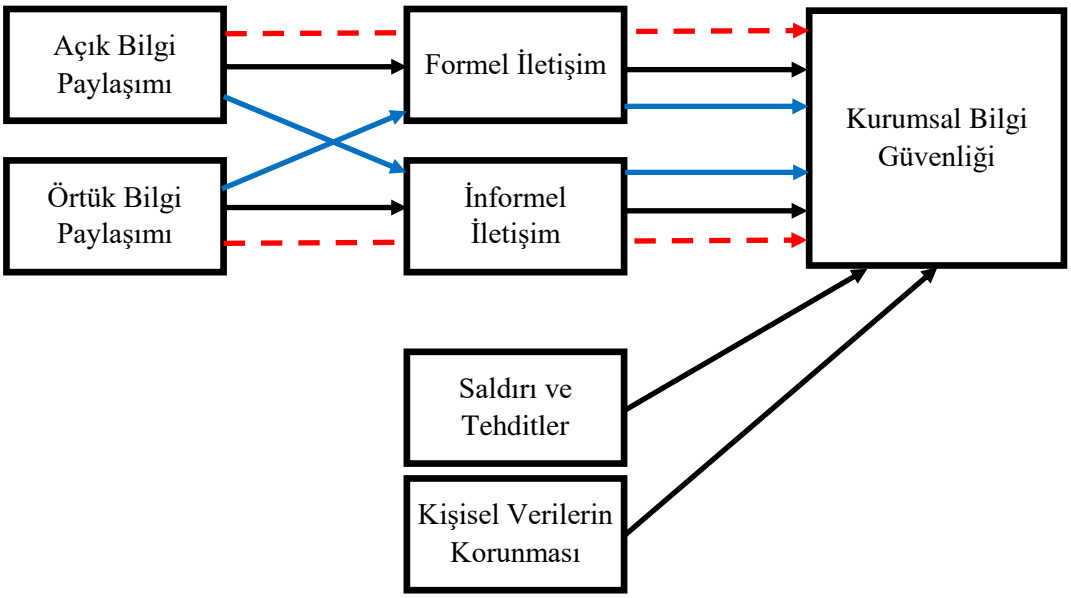
Tablo 2. Araştırma Soruları, Örneklem, Veri Toplama Araçları ve Veri Analiz Yöntemleri

Araştırma Sorusu	Örneklem	Veri Toplama Araçları	Veri Analiz Yöntemleri
Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği farkındalığına, kişisel bilgi güvenliği farkındalığına, örgütsel iletişime ve örgütsel bilgi paylaşımına ilişkin algıları ne düzeydedir?	479 Akademik ve idari personel	Kişisel Bilgi Formu Bilgi Güvenliği Ölçeği Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği Bilgi Paylaşımı Ölçeği Örgütsel İletişim Ölçeği	Betimsel analizler (frekans, yüzde, ortalama,)
Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği farkındalığı, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı demografik değişkenlere (cinsiyet, yaş, hizmet süresi, İnternette/ sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı) göre anlamlı farklılık göstermekte midir?			Bağımsız Gruplar t-testi Tek Yönlü Varyans Analizi (ANOVA) Scheffe testi Cohen d ve eta kare (η2) değeri
Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği ile kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı arasında nasıl bir ilişki vardır?			Korelasyon Analizi Regresyon Analizi Yapısal Eşitlik Modellemesi Aracılık Analizi Bootstrap Yöntemi
Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliğinin veri madenciliği yöntemleri ile tahmin başarımı nedir?			Veri madenciliği tahmin edici modeller Yapay Sinir Ağları Destek Vektör Makineleri K- En Yakın Komşu Algoritması Rastgele Orman Yöntemi

3.1. Araştırmanın Modeli

Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliğinin, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı bağlamında değerlendirilmesinin amaçlandığı bu çalışma nicel araştırma yöntemlerinden tarama modeliyle tasarlanmıştır. Tarama modeli, bir grubun belirli özelliklerini belirlemek için kullanılan araştırma yöntemi olarak tanımlanabilir (Büyüköztürk, Kılıç Çakmak, Akgün, Karadeniz ve Demirel, 2012: 14). Bu çalışmada kurumsal bilgi güvenliği ile kişisel bilgi güvenliği farkındalığı (kişisel verilerin korunması, saldırı ve tehditler farkındalığı), örgütsel iletişim (formel ve informel iletişim) ve örgütsel bilgi paylaşımı (açık ve örtük bilgi paylaşımı) değişkenleri arasındaki ilişkilerin belirlenmesi amaçlanmaktadır. Bu ilişkilerin belirlenmesinde ilişkisel tarama modeli benimsenmiştir. İlişkisel tarama modeli iki veya daha çok değişken arasındaki birlikte değişimin varlığını ve derecesini belirlemeyi amaçlayan tarama modelidir (Karasar, 2010: 81).

Araştırma değişkenleri arasında kabul edilen ilişkilere yönelik varsayımsal model Şekil 2'de sunulmuştur.



(Kesik çizgiler aracı değişken üzerinden ilişkiyi göstermektedir. Doğru çizgiler ise doğrudan ilişkiyi göstermektedir.)

Şekil 2. Değişkenler Arasındaki İlişkilere Yönelik Varsayımsal Model

Araştırma kapsamında "Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği ile kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı arasında nasıl bir ilişki vardır?" sorusuna yönelik olarak geliştirilen hipotezler aşağıda maddeler halinde sıralanmıştır:

H1: Saldırı ve tehditlere yönelik farkındalık kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler.

H2: Kişisel verilerin korunmasına yönelik farkındalık kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler.

H3: Formel iletişim kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler.

H4: İnformel iletişim kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler.

H5: Açık bilgi paylaşımı kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler.

H6: Örtük bilgi paylaşımı kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler.

H7: Açık bilgi paylaşımı formel iletişim düzeyini pozitif ve anlamlı etkiler.

H8: Açık bilgi paylaşımı informel iletişim düzeyini pozitif ve anlamlı etkiler.

H9: Örtük bilgi paylaşımı formel iletişim düzeyini pozitif ve anlamlı etkiler.

H10: Örtük bilgi paylaşımı informel iletişim düzeyini pozitif ve anlamlı etkiler.

H11: Açık bilgi paylaşımı kurumsal bilgi güvenliğini dolaylı etkiler.

H12: Örtük bilgi paylaşımı kurumsal bilgi güvenliğini dolaylı etkiler.

H13: Formel iletişimin açık bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi vardır.

H14: İnformel iletişimin açık bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi vardır.

H15: Formel iletişimin örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi vardır.

H16:İnformel iletişimin örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi vardır.

3.2. Eğitsel Veri Madenciliği

Bu tez çalışmasında üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği puanı veri madenciliği yöntemleri ile tahmin edilmiştir. Veri madenciliği, büyük miktarda verinin yaygın olarak bulunması ve bu verilerin yararlı bilgiye dönüştürülmesine yönelik ihtiyaç nedeni ile son yıllarda bilgi endüstrisi ve toplumda büyük ilgi görmektedir (Han ve Kamber, 2011: 1). Bilgi teknolojisinde yaşanan gelişmelerin bir sonucu olan (Han ve Kamber, 2011: 1) veri madenciliği, büyük miktarda veriden gizli, örtük ve anlamlı bilgiler elde etme yöntemidir (Kamath ve Kamat, 2016: 2). Bilgisayar bilimi, makine öğrenimi ve istatistik alanlarındaki becerileri birleştiren veri madenciliği büyük veri tabanının, gelişmiş analitik becerilerin ve alan bilgisinin bir birleşimini kullanarak anlamlı ve faydalı bilgiler ortaya çıkartmaktadır (Kamath ve Kamat, 2016: 2-3). Veri madenciliği işletme, hükümet, finansal hizmetler, bankacılık, pazarlama, biyoloji, tıp, istihbarat, bilim, mühendislik, eğitim gibi alanların çoğunda uygulama alanına sahiptir (Kamath ve Kamat, 2016: 3: Sivakumar, Venkataraman ve Selvaraj, 2016: 1). Eğitim ortamlarındaki veri madenciliği eğitsel veri madenciliği olarak ifade edilmektedir (Devasia, Vinushree ve Hegde, 2016: 1).

Eğitsel veri madenciliği, eğitim ortamlarından gelen özel veri türlerini keşfetmek için teknikler geliştirmek ve bu yararlı bilgileri eğitim kurumlarının büyümesi için kullanan bir disiplindir (Kamath ve Kamat, 2016: 7). Benzer bir ifadeyle eğitsel veri madenciliği farklı eğitim verisi türleri üzerinde istatistiksel, makine öğrenimi ve veri madenciliği algoritmalarından yararlanan bir alandır (Romero ve Ventura, 2010: 601). Eğitsel veri madenciliği büyük miktarda yapılandırılmamış ham verileri analiz ederek eğitim araştırmaları ve uygulamaları üzerinde potansiyel olarak büyük bir etkisi olabilecek faydalı bilgilere dönüştürür (Pratiyush ve Manu, 2016: 1; Romero ve Ventura, 2010: 601). Veri madenciliği yöntemleri kullanılarak araştırmacılar, eğitim yazılımlarından bireysel öğrenme, bilgisayar destekli işbirlikçi öğrenme, bilgisayara uyarlanabilir test (ve daha geniş anlamda test etme) ve öğrenci başarısızlığı veya derslerde kalıcılık ile ilişkili faktörler dahil olmak üzere çeşitli alanları incelemektedirler (Romero ve Ventura, 2010: 601). Daha iyi ve daha akıllı öğrenme teknolojisi tasarlamak, öğrencileri ve eğitimcileri daha iyi bilgilendirmek için eğitsel veri madenciliği kullanılabilir (Baker, 2014: 78). Eğitim ortamlarından gelen veriler, veri madenciliği teknikleri kullanılarak analiz edilmektedir (Kamath ve Kamat, 2016: 7; Pratiyush ve Manu, 2016: 1).

Veri madenciliği tanımlayıcı ve tahmin edici modeller olarak iki kategoride sınıflandırılabilir. Tanımlayıcı modeller, veri tabanındaki verilerin genel özelliklerini karakterize etmektedir (Han ve Kamber, 2011: 21) ve mevcut veri kümesine dayalı olarak, anlamlı tanımlayıcı bilgiler üretmektedir (Kantardzic, 2011: 2-3). Tahmin edici modeller ise mevcut veriler üzerinden çıkarımlar gerçekleştirmektedir (Han ve Kamber, 2011: 21). Tahmin edici modeller de amaç, verilerin diğer yönlerinin bazı kombinasyonlarından (geleneksel istatistiksel analizdeki bağımsız değişkenlere benzer şekilde yordayıcı değişkenler), verilerin tek bir yönünü (geleneksel istatistiksel analizdeki bağımlı değişkenlere benzer tahmin edilen değişken) çıkarabilen bir model geliştirmektir (Baker ve Inventado, 2014: 63). Tahminin amacı, verilerin diğer yönlerinin (tahmin değişkenleri) bazı kombinasyonlarından verilerin (öngörülen değişken) bir hedef niteliğini veya tek yönünü çıkarmaktır (Romero ve Ventura, 2013: 21). Tahmin, sınırlı bir veri kümesi için çıktı değişkeni etiketlere sahip olmayı gerektirir; burada bir etiket, belirli durumlarda tahmin edilen değişkenin değeri hakkında bazı güvenilir temel doğruluk bilgilerini temsil eder. (Baker ve Inventado, 2014: 63). Tez çalışmasında veri madenciliğinin tahmin edici modelleri kullanılmıştır.

Tahmin edici modellerde Karar Ağaçları, Destek Vektör Makineleri, Yapay Sinir Ağları, Naive Bayes, K-En Yakın Komşu gibi birçok teknik kullanılmaktadır. Bu çalışmada tahmin edici modellerden, Yapay Sinir Ağları, Destek Vektör Makineleri, K-En Yakın Komşu ve Rastgele Orman algoritmaları kullanılmıştır. Tez çalışması kapsamında kurumsal bilgi güvenliği puanı çıkış değişkeni; saldırı ve tehditler, kişisel verilerin korunması, formel iletişim, informel iletişim, açık bilgi paylaşımı, örtük bilgi paylaşımı puanları giriş değişkeni olarak belirlenmiştir.

Yapay Sinir Ağları, başlangıçta, nöronların hesaplamalı analoglarını geliştirmeye ve test etmeye çalışan psikologlar ve nörobiyologlar tarafından önerilmiştir (Han ve Kamber, 2011: 327). Yapay Sinir Ağları, çok verimli bir algoritmadır ve nispeten basit bir eğitim sürecine sahiptir (Matej ve Miroslav, 2016: 301). Her bir sinir ağı, her bağlantının kendisiyle ilişkili bir ağırlığı olan bir dizi bağlı giriş/çıkış birimidir. Öğrenme aşamasında ağ, girdi gruplarının doğru sınıf etiketini tahmin edebilmek için ağırlıkları ayarlayarak öğrenir. Gürültülü verilere karşı yüksek tolerans içeren Yapay Sinir Ağları sınıflandırma ve tahmin modelleri için kullanışlıdır (Han ve Kamber, 2011: 327).

Destek Vektör Makineleri, veri madenciliği tekniklerinden biridir ve hem regresyon hem de sınıflandırma için kullanılabilir (Pratiyush ve Manu, 2016: 1). Temeli 1960'lara dayanan Destek Vektör Makineleri hakkındaki ilk makale 1992 yılında Vladimir Vapnik ve meslektaşları Bernhard Boser ve Isabelle Guyon tarafından sunulmuştur. Destek Vektör Makinelerinin karmaşık doğrusal olmayan karar sınırlarını modelleme yeteneği oldukça hassastır (Han ve Kamber, 2011: 337).Yapay Sinir Ağları ile ilişkili olan Destek Vektör Makineleri, büyük potansiyele ve üstün performansa sahiptir ayrıca sıklıkla tahmin amacıyla kullanılmaktadır (Kartal, 2020: 1404).

K-En Yakın Komşu Yöntemi, ilk olarak 1950'lerin başında tanımlanmış ve 1960'lardan sonra popülerlik kazanmıştır. Örüntü tanıma alanında yaygın olarak kullanılan (Han ve Kamber, 2011: 348) K-En Yakın Komşu algoritması, analoji yoluyla yani verilen bir test örneğini ona benzer eğitim örnekleriyle karşılaştırarak öğrenmeye dayanır (Akhtar, 2016: 33). Sınıfları belli olan bir örnek kümesinde yer alan gözlem değerlerinden faydalanarak eklenecek olan yeni bir gözlemin hangi sınıfa ait olduğunu belirlemek amacıyla kullanılmaktadır (Özkan, 2016: 141).

Rastgele Orman Yöntemi, çok sayıda karar ağacının bir araya getirilmesine dayanan bir sınıflandırma ve regresyon yöntemidir. Denetimli bir öğrenme probleminde bir tahmin kuralı oluşturmak ve değişkenlerin yanıtını tahmin etme yeteneklerine göre değerlendirmek ve sıralamak amacı ile kullanılmaktadır (Boulesteix, Janitza, Kruppa ve König, 2012: 493-494). Hızlı ve esnek olan (Ziegler ve König, 2014: 55) Rastgele Orman yöntemi değişken sayısının gözlem sayısından çok daha fazla olduğu ortamlarda mükemmel performans göstermektedir (Boulesteix, Janitza, Kruppa ve König, 2012: 493-494).

3.3. Evren ve Örneklem

Araştırma sonuçlarının genellenmesinin istendiği elemanların tümü olarak tanımlanan evren, araştırmacının amacı doğrultusunda belirlenmektedir (Karasar, 2010: 109). Bu çalışmanın evrenini, Türkiye'nin doğusunda yer alan bir üniversitede görev yapan 4105 akademik ve idari personel oluşturmaktadır. Belli bir evrenden, evreni temsil ettiği kabul edilen belli kurallara göre seçilmiş küme, örneklem olarak tanımlanabilir (Karasar, 2010: 110). Örneklemin seçiminde seçkisiz olmayan örnekleme yöntemlerinden biri olan elverişli/uygun örnekleme yöntemi kullanılmıştır. Elverişli örnekleme yöntemi olarak da adlandırılan uygun örnekleme yöntemi zaman, para ve işgücü kaybını en aza indirmeyi amaçlayan örnekleme yöntemidir (Büyüköztürk vd., 2012). Bu

çalışmada örneklemin, evreni temsil etmesi açısından %95 güven düzeyinde, %4 sapma miktarı ile 522 katılımcıdan veri toplanması yeterlidir (Çıngı 1994, Aktaran: Büyüköztürk vd., 2012). Araştırma kapsamında hedeflenen örneklem sayısına ulaşmak için basılı ve çevrimiçi anket formları Türkiye'nin doğusunda yer alan bir üniversitede görev yapan akademik ve idari personele uygulanmıştır. Verilerin 401 tanesi basılı, 126 tanesi ise çevrimiçi formlardan toplanmıştır. Ancak eksik ve hatalı doldurulan, 48 anket formu değerlendirme dışı bırakılmıştır. 479 veri üzerinde analizler gerçekleştirilmiştir. Tablo 3'te araştırmaya katılan akademik ve idari personelin demografik özellikleri sunulmuştur.

Tablo 3. Katılımcıların Demografik Bilgileri

Değişken	**Gruplar**	**N**	**%**
Cinsiyet	Kadın	304	63.5
	Erkek	175	36.5
Medeni Hal	Evli	380	79.3
	Bekar	99	20.7
Yaş	35 yaş altı	121	25.3
	30-44	152	31.7
	45-55	139	29.0
	55 ve üzeri	67	14.0
Hizmet Süresi	5 yıldan az	67	14.0
	5-10 yıl	96	20.0
	11-20 yıl	109	22.8
	21-30 yıl	129	26.9
	30 yıl ve üzeri	78	16.3
Eğitim Düzeyi	Lise	26	5.4
	Ön Lisans	33	6.9
	Lisans	88	18.4
	Yüksek Lisans	74	15.4
	Doktora	258	53.9
İnterneti Kullanma Amacı	Gazete okuma/haber izleme/bilgi edinme	365	76.2
	Alışveriş	254	53.0
	Sosyal Ağ	244	50.9
	Konuşma/Mesajlaşma	208	43.4
	Müzik dinleme	203	42.4
	Film/video izleme	189	39.5
	Akademik çalışmalar/Araştırma yapma	174	36.4
	Kurumsal işlemler	85	17.7
	Oyun oynama	61	12.7
Sosyal Ağ Kullanma Düzeyi	Düşük	162	33.8
	Orta	244	50.9
	Yüksek	73	15.2
İnternette/Sosyal Ağ Sitelerinde Paylaşılan Kişisel Bilgiler	E-posta adresi	300	62.6
	Telefon numarası	75	15.7
	Doğum tarihi	92	19.2
	Kişisel fotoğraf	229	47.8
	Kişisel video	66	13.8
İnternette/ sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı	Ayda birkaç defa	79	16.5
	Ayda bir	67	14.0
	Yılda birkaç defa	115	24.0
	Yılda bir defa	67	14.0
	Kontrol etmiyorum	151	31.5
Toplam		479	100

Tablo 3 incelendiğinde, araştırmaya katılan 479 akademik ve idari personelin %63.5'nin kadın, %36.5'nin erkek olduğu görülmektedir. Araştırmaya katılan akademik ve idari personelin yaşa göre dağılımları incelendiğinde %31.7'si 30-44 yaş, %14.0 ise 55 yaş ve üzerindedir ve katılımcıların %14.0'ü 5 yıldan az, %26.9'u 21-30 yıl hizmet süresine sahiptir. Araştırmaya katılan katılımcıların eğitim düzeylerine göre dağılımları incelendiğinde %5.4'nün lise ve %53.9'nun doktora mezunu olduğu görülmektedir. Katılımcılar İnterneti en fazla okuma/haber izleme/bilgi edinme (%76.2) için kullanırken en az oyun oynama (12.7) amacıyla kullanmaktadır. Araştırmaya

katılan akademik ve idari personelin %50.9'u sosyal ağları orta düzey kullandığı, İnternet/ Sosyal ağ sitelerinde en fazla e-posta adresini (62.6) paylaştığı, yılda birkaç defa (24.0) İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol ettiği belirlenmiştir.

3.4. Veri Toplama Süreci

Bu araştırmada, Bilgi Güvenliği Ölçeği (Gerçeker, 2012), Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği (Keser ve Güldüren, 2015), Örgütsel İletişim Envanteri (Tuna, 2008) ve Bilgi Paylaşım Ölçeği (Aslan, 2014) kullanılmıştır. Ölçekler ve envanter araştırmada kullanılmadan önce ölçekleri ve envanteri geliştiren araştırmacılardan izin alınmıştır. Veri toplama araçlarının kullanımı için gerekli izinler alındıktan sonra araştırmaya başlamak için etik kurul izni, tez öneri kabul onayı ve ölçek uygulama izni ilgili kurumlardan alınmıştır. Alınan etik kurul izni EK 2'de, uygulama izni ise EK 1'de sunulmuştur. Ayrıca Örgütsel İletişim Envanteri'nin standardizasyon işlemlerinin gerçekleştirilebilmesi için Türkiye'nin doğusunda yer alan iki üniversiteden anket uygulama izni alınmıştır. Alınan etik kurul izni EK 1'de, uygulama izni ise EK 1'de sunulmuştur. Ancak pandemi sürecinde yaşanan aksaklıklar nedeniyle etik kurul izni güncellenmiştir. Alınan ek izin EK 2'de sunulmuştur.

Uygulama Süreci: Verilerin toplanması için gerekli izinler alındıktan sonra ölçeklerin çevrimiçi ve basılı formları oluşturulmuştur. Basılı formlar Türkiye'nin doğusunda yer alan bir üniversitede Türkiye'nin doğusunda yer alan tüm fakülte, yüksekokul, daire başkanlıkları, birimler ziyaret edilerek katılımcılara elden dağıtılmıştır. Veri toplama sürecinde etik değerlere bağlı kalınarak gönüllü katılımcılara veri toplama araçları uygulanmıştır. Katılımcılara istedikleri zaman ölçeği doldurmayı bırakabilecekleri belirtilmiştir.

Araştırmacının Sorumluluğu: Pandemi nedeniyle uzaktan eğitim sürecinin devam etmesi, esnek çalışma uygulaması, kronik rahatsızlığı olan çalışanların idari izinli olmaları gibi nedenlerden dolayı fakülte, yüksekokul, daire başkanlıkları ve birimler belirli aralıklarla birden fazla kez ziyaret edilmiştir. Ayrıca veri toplama araçlarının basılı formunu doldurmak istemeyen katılımcılara çevrimiçi form gönderilmiş, pandemi kurallarına da uyarak daha fazla katılımcıya ulaşılmaya çalışılmıştır. Veri toplama araçları uygulanmadan önce araştırmacı kendini tanıtmış, araştırmanın içeriğinden bahsetmiş, izin yazıları katılımcılara gösterilmiştir. Araştırmaya katkılarından dolayı katılımcılara teşekkür edilmiştir. Araştırmacı katılımcıların ölçek formlarını doldurması sırasında yanlılık olmaması için herhangi bir müdahalede bulunmamış, zaman ve mekan sınırlaması getirmemiştir. Ayrıca toplanacak verilerin üçüncü kişilerle veya kurum yöneticileriyle paylaşılmayacağı belirtilmiştir.

3.5. Verilerin Analizi

Araştırma sonucunda elde edilen veriler, veri analiz programları ile analiz edilmiştir. Elde edilen verilerin analizine başlamadan önce kayıp ve uç değerler incelenmiş, normallik testleri gerçekleştirilmiştir. Verilerin normal dağılımının belirlenmesi amacıyla basıklık ve çarpıklık değerlerine bakılabilir (Tabachnick ve Fidell, 2007: 79). Verilerin normal dağılımının belirlenmesine yönelik basıklık (Kurtosis) ve çarpıklık (Skewness) değerleri hesaplanmış ve elde edilen değerler Tablo 4'de sunulmuştur.

Tablo 4. Araştırmada Kullanılan Ölçeklerden Elde Edilen Ortalama Puanlar ve Normallik Değerleri

Ölçekler	N	$\bar{X}$	Ss	Skewness	Kurtosis
Kurumsal Bilgi Güvenliği	479	89.873	14.051	0.099	0.246
Kurumsal Bilgi Güvenliği Ölçeği Alt Boyutları					
Bilgi Güvenliği Kültürü Boyutu	479	17.073	3.539	-0.104	0.206
Bilgi Güvenliği Uygulaması Boyutu	479	19.964	3.645	-0.032	0.307
Bilgi Güvenliği Yaklaşımı Boyutu	479	13.672	2.648	0.073	-0.158
Bilgi Güvenliği Yönetimi Boyutu	479	27.559	4.854	0.130	-0.036
Bilgi Güvenliğinde Gizlilik Boyutu	479	11.603	2.099	-0.677	-0.322
Bilgi Güvenliği Farkındalığı Düzeyi Belirleme	479	118.605	19.698	0.217	-0.210
Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği Alt Boyutları					
Saldırı ve Tehditler Boyutu	479	52.267	10.498	0.085	-0.262
Kişisel Verilerin Korunması Boyutu	479	68.106	10.916	0.049	-0.266
Örgütsel İletişim	479	41.770	7.484	-0.075	-.0.095
Örgütsel İletişim Ölçeği Alt Boyutları					
Formel İletişim Boyutu	479	41.770	7.484	-0.075	-0.095
İnformel İletişim Boyutu	479	11.620	2.277	0.223	-0.218
Bilgi Paylaşımı	479	37.633	6.116	0.453	0.751
Bilgi Paylaşım Ölçeği Alt Boyutları					
Açık Bilgi Paylaşımı Boyutu	479	13.315	2.693	0.219	0.016
Örtük Bilgi Paylaşımı Boyutu	479	24.317	4.131	0.317	0.381

Tablo 4'te yer alan basıklık ve çarpıklık değerleri incelendiğinde, +1 ile -1 arasında değiştiği görülmektedir. Tabachnick ve Fidell (2007: 79), basıklık ve çarpıklık değerinin -1 ile +1 arasında değişmesinin verilerin normal dağılım gösterdiğini kabul etmektedir. Basıklık ve çarpıklık değerleri hesaplandıktan sonra frekans, yüzde, ortalama gibi betimsel analizler gerçekleştirilmiştir. Ölçeklerden elde edilen aritmetik ortalamaların yorumlanmasında Tablo 5'de yer alan aralıklar dikkate alınmıştır. Ölçeklerin aralık genişliği hesaplanırken Tekin (2004) "dizi genişliği/yapılacak grup sayısı" (5-1=4 => 4/5= 0.80) formülünden faydalanılmıştır.

Tablo 5. Ölçek Aralık Genişliği

Cevap Seçeneği	Puan Aralığı	Puan Düzeyi
Kesinlikle katılmıyorum/Asla	1.00-1.80	Çok Düşük
Katılmıyorum/Nadiren	1.81-2.60	Düşük
Kararsızım/Bazen	2.61-3.40	Orta
Katılıyorum/Sık sık	3.41-4.20	Yüksek
Kesinlikle katılıyorum/ Sürekli olarak	4.21-5.00	Çok Yüksek

Değişkenler arasındaki ilişkilerin belirlenmesi amacıyla korelasyon testi yapılmıştır. Korelasyon katsayısı +1 ile -1 arasında değişmektedir ve +1 yüksek pozitif ilişkiyi, -1 yüksek negatif ilişkiyi, 0 ise ilişki olmadığını göstermektedir (Kline, 1994: 3). Büyüköztürk (2012: 32), korelasyon katsayılarını 0-0.30 düşük, 0.30-0.70 orta, 0.70-1.00 yüksek olarak yorumlamaktadır.

Verilerin normal dağılması nedeniyle ikili gruplar arasında anlamlı farklılıkların olup olmadığını belirlemek için Bağımsız Gruplar t-testi, ikiden fazla gruplar arasında anlamlı farklılıkların olup olmadığını belirlemek için Tek Yönlü Varyans Analizi (ANOVA) testi kullanılmıştır. İkiden fazla gruplardan, grupların homojen dağılması nedeniyle farklılığın kaynağının belirlenmesi amacıyla post-hoc analizlerinden Scheffe testi kullanılmıştır. Çalışmada etki büyüklüğünün belirlenmesi için Cohen d (d) ve eta kare ($\eta 2$) değeri hesaplanmıştır. Bağımsız değişkenin, bağımlı değişkendeki toplam varyansın açıklanma düzeyi olarak tanımlanan eta kare ($\eta 2$) değeri, 0.00-1.00 aralığında değer alır. Bu değerler ".01" değeri küçük, ".06" değeri orta ve ".14" değeri geniş etki büyüklüğü olarak değerlendirilmektedir (Büyüköztürk, 2014: 44). Cohen (1988) yöntemi kullanılarak hesaplanan d değerinin etki büyüklüğü, $d<0.02$ "küçük" etki, $0.02<d<0.08$ "orta" etki ve $d>0.08$ "büyük" etki olarak sınıflandırılmaktadır (Cohen, 1988).

Kurumsal bilgi güvenliği üzerinde bilgi güvenliği farkındalığı, örgütsel iletişim, örgütsel bilgi paylaşımının ve yordayıcılıklarının belirlenmesi amacıyla regresyon analizi gerçekleştirilmiştir. Regresyon analizi, aralarında ilişki olan iki veya daha fazla değişken arasındaki ilişkinin matematiksel eşitlik ile açıklaması olarak tanımlanabilir (Büyüköztürk, 2012: 91).

Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliğinin, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı bağlamında değerlendirilmesinin amaçlandığı bu çalışmada, kuramsal yapının test edilmesi ve ilişkilerin ortaya çıkartılması amacı ile yapısal eşitlik modellemesi yapılmıştır. Yapısal eşitlik modellemesi (YEM), tek bir istatistiksel teknikten ziyade bir dizi ilişkili işlemleri ifade etmektedir (Kline, 2015: 9). Yapısal eşitlik modelini bir dizi değişken arasındaki ilişkileri açıklayan teorik modelleri test etmek için kullanılmaktadır (Hu ve Bentler, 1999: 2). Ayrıca değişkenler arasındaki nedensellik ilişkilerin geçerliliğinin de test edilmesine imkan tanımaktadır (Meydan ve Şeşen, 2015: 17). YEM'in ortaya çıkmasında, yol analizi, faktör analizi ve eşzamanlı eşitlik modelleri rol oynamıştır (Şen, 2020: 1) ve YEM'in temel amacı önceden kararlaştırılan ilişki ağının elde edilen verilerle doğrulanıp doğrulanmayacağını ortaya çıkarmaktır (Şen, 2020: 4). YEM'in gerçekleştirilmesinde model belirleme, tanımlama, kestirim, modelin testi ve değerlendirilmesi ve gerekmesi durumunda model modifikasyonu adımlarının takip edilmesi gerekmektedir (Şen, 2020: 16; Çokluk, Şekercioğlu ve Büyüköztürk, 2016: 272). Model belirleme YEM sürecinin en önemli adımıdır ve teorik çerçeveye göre oluşturulmaktadır (Kline, 2015: 119). YEM'de, değişkenler modeldeki rollerine göre içsel, dışsal ve aracı değişken olarak sınıflandırılmaktadır. Bu çalışmada kurumsal bilgi güvenliği içsel (bağımlı) değişken, kişisel bilgi güvenliği farkındalığı (saldırı ve tehditler, kişisel verilerin korunması), örgütsel bilgi paylaşımı (açık bilgi paylaşımı ve örtük bilgi paylaşımı) dışsal (bağımsız) değişken olarak belirlenmiştir. Örgütsel iletişim (formel iletişim ve informel iletişim), kurumsal bilgi güvenliğini doğrudan veya dolaylı olarak etkileyebileceği için bağımlı ve bağımsız değişken olarak ifade edilmiştir. Aynı zamanda örgütsel iletişim (formel iletişim ve informel iletişim) bağımlı ve bağımsız değişkenler arasındaki ilişkiye aracılık etmesi nedeniyle aracı değişkendir. Aracı değişken, bir değişkenin etkisinin başka bir değişkene ileten davranışsal, biyolojik, psikolojik veya sosyal yapılardır (MacKinnon, Fairchild ve Fritz, 2007: 595). Diğer bir deyişle aracı değişken bağımlı ve bağımsız değişkenler arasındaki ilişkiye aracılık eden değişken olarak tanımlanabilir (Şen, 2020: 7).

Bu çalışmada örgütsel iletişim (formel iletişim ve informel iletişim), kurumsal bilgi güvenliği ve örgütsel bilgi paylaşımı (örtük bilgi paylaşımı ve açık bilgi paylaşımı) ile arasındaki ilişkide aracılık rolünü belirlemek için aracılık analizi gerçekleştirilmiştir. Aracılık analizi, bir değişkenin diğerini etkilediği süreci veya mekanizmayı açıklayabilmenin bir yöntemi olarak tanımlanabilir (MacKinnon, Fairchild ve Fritz, 2007: 595). Bağımlı ve bağımsız değişken arasındaki doğrudan ilişkiden ziyade ilk bakışta görülmeyen etkileri inceleyen aracılık analizi, bağımlı ve bağımsız değişken arasındaki dolaylı ilişkiyi incelemektedir (Yılmaz ve Dalbudak, 2018: 518).

Aracılık modeli analizinde çağdaş yaklaşımlar arasında yer alan bootstrap yöntemi dolaylı etki değerinin hesaplanması ve hesaplanan değerlerden çıkarımlar yapılmasına odaklanmaktadır. Bootstrap analizi sonucunda dolaylı etkinin anlamlı olması durumunda aracılık modeli doğrulanmış olarak kabul edilmekte ve farklı herhangi bir test yapılmasına gerek duyulmamaktadır (Gürbüz, 2021: 58). Bootstrap analizi orijinal veri setinde yer alan örneklerden rastgele yeni örnek veri setleri oluşturularak, hesaplamaların yeni örneklem setlerinden yapılmasına dayanmaktadır. Yinelenerek

elde edilen bu örnek veri setlerinden dolaylı etki değeri hesaplanır (Efron ve Tibshirani, 1994: 18). Bootstrap analizi ile dolaylı etki değerinin %95 güven aralığında alt ve üst sınırları belirlenir (Gürbüz, 2021: 61). Aracılık analizinde çağdaş yaklaşımlar arasında yer alması, karmaşık modeller için geçerli ve güvenilir sonuçlar üretmesi, (Efron ve Tibshirani, 1994: 18; Gürbüz, 2021: 61) nedeni ile bu çalışmada Bootstrap analizi kullanılmıştır.

Yapısal eşitlik uygulamalarında modelin doğrulanması için bazı uyum indeksleri kullanılmaktadır (Hu ve Bentler, 1999: 2). Tablo 6'da uyum indekslerinin mükemmel ve kabul edilebilir uyum referans değerleri sunulmuştur.

Tablo 6. YEM Uyum İndeksleri

Uyum İndeksi	Mükemmel Değerler	Uyumlu Değerler
p	p<.01	p<.05
χ2/df	0≤χ2/df≤3	3≤ χ2/df≤5
RMR	0<RMR≤0.5	0.5< RMR < 1
SRMR	0<SRMR≤0.5	0.5<SRMR < 1
GFI	0.95≤GFI≤1.00	0.90≤GFI≤0.95
AGFI	0.90≤AGFI≤1.00	0.85≤AGFI≤0.90
NFI	0.95≤NFI≤1.00	0.90≤NFI≤0.95
TLI	0.95≤TLI≤1.00	0.90≤TLI≤0.95
CFI	0.95≤CFI≤1.00	0.90≤CFI≤0.95
RMSEA	0≤RMSEA≤0.05	0.05≤RMSEA≤0.08

(Hu ve Bentler, 1999: 13-15; Sümer, 2000: 72; Kline, 2015).

YEM'de uyum indekslerinden sonra modelin modifikasyonu hakkında bilgi veren modifikasyon indeksleri incelenmektedir. Model modifikasyon indeksleri, modele belirli bir parametre eklenirse kikare (χ2) değerinin düşeceği miktarın ölçüsünü göstermektedir (Şen, 2020: 34). Modifikasyonlar, gözlenen ve gizil değişkenler arasında önerilen yeni bağlantıları kapsamaktadır (Meydan ve Şeşen, 2015: 41). Bu modifikasyon indeksi değerleri modelin uyumunu arttırmak için eklenebilecek model parametrelerini önermektedir (Şen, 2020: 34). Uyum indekslerinin iyileştirilmesi amacıyla kapsam geçerliliği de göz önünde bulundurularak gerekli durumda modifikasyonlar gerçekleştirilmiştir.

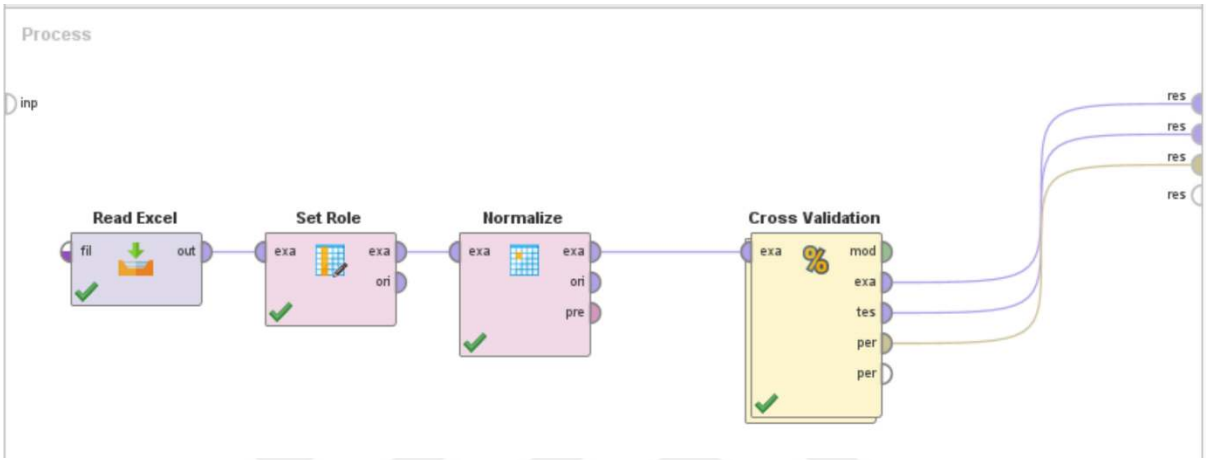
3.6. Veri Madenciliği Analiz Süreci

Üniversite çalışan akademik ve idari personelin, bilgi güvenliği farkındalığı (saldırı ve tehditler, kişisel verilerin korunması), örgütsel iletişim (formel iletişim, informel iletişim) ve bilgi paylaşımı (açık bilgi paylaşımı, örtük bilgi paylaşımı) verileri ile kurumsal bilgi güvenliğinin tahmin başarımı analiz edilmiştir. Veri madenciliği bir süreç olarak değerlendirilmektedir (Özkan, 2016: 27). Veri analizi gerçekleştirilmeden önce veri temizleme, veri bütünleştirme, veri dönüştürme ve RapidMiner programında model oluşturma işlemleri gerçekleştirilmiştir.

Veri temizleme, eksik, hatalı ve tutarsız verilerin veri kümesinden atılması sürecidir (Özkan, 2016: 27). Veri bütünleştirme sürecinde, farklı veri tabanlarından veya kaynaklarda yer alan verilerin bir araya getirilmesidir (Özkan, 2016: 28). Çevrimiçi ve basılı formlar kullanılarak elde edilen veriler Microsft Excel programına aktarılmıştır. Elde edilen veriler, veri madenciliği çözümlemeleri için uygun olmayabilir. Bu nedenle veri dönüştürme işlemi ile verilerin veri madenciliği analizleri için uygun biçime dönüştürülmüştür (Özkan, 2016: 29). Bu tez çalışmasında kullanılan ölçek verileri ölçek yönergelerinde yer alan biçimde 1-5 şeklinde derecelendirilerek düzenlenmiştir.

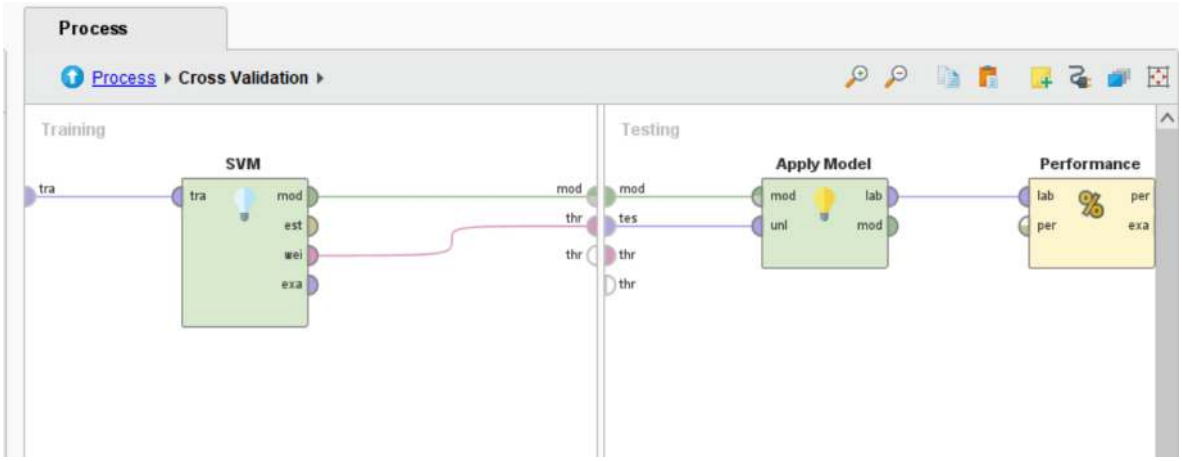
Veri madenciliği analizleri açık kaynak kodlu, sürükle bırak yöntemi ile birbirine bağlanan operatörler sayesinde çalışan (Çelik, Akçetin ve Gök, 2017: 3), RapidMiner programında gerçekleştirilmiştir. Kullanımı kolay bir ara yüze sahip olan RapidMiner programı, farklı dosya biçimlerinde veri giriş ve çıkışına imkan tanımaktadır (Hofmann ve Klinkenberg, 2016: 19).

Analiz işlemleri için Rapidminer programında oluşturulan modeller Şekil 3'te görülmektedir ve oluşturulan modeller Yapay Sinir Ağları, destek vektör makinaları, K-En Yakın Komşu algoritmalarına göre uyarlanmıştır. Modelde Read Excel, Set Role, Normalize, Cross Validation ve Cross Validation operatörü altında ise SVM, Apply Model ve Performance operatörleri kullanılmıştır.



Şekil 3. Rapidminer Model Yapısı

Read Excel operatörü ile Microst Excelde kayıtlı olan veriler RapidMiner programına aktarılmıştır. Set Role operatörü ile bağımlı değişken (tahmin edilen değişken) ve açıklayıcı değişkenlerine (girdi değişkenleri) ilişkin ayarlamalar gerçekleştirilmiştir. Bu tez çalışmasında bağımlı değişken kurumsal bilgi güvenliği; açıklayıcı değişkenler ise saldırı ve tehditler, kişisel verilerin korunması, formel iletişim, informel iletişim, açık bilgi paylaşımı ve örtük bilgi paylaşımı olarak belirlenmiştir. Normalize operatörü kullanılarak verilerin normalize işlemi gerçekleştirilmiştir. Bu tez çalışmasında veriler 0-1 aralığında normalize edilmiştir. Normalize işlemi gerçekleştirilirken "Range Transformation" yöntemi kullanılmıştır. Cross Validation iç içe operatörünün altında eğitim ve test verilerine ilişkin operatörler yer almaktadır.



Şekil 4. Rapidminer Model Yapısı

Tez çalışmasında kullanılan Destek Vektör Makineleri, Yapay Sinir Ağları, K-En Yakın Komşu, Rastgele Orman algoritmalarında da aynı süreç izlenmiş, sadece eğitim sürecindeki operatörler SVM, Neural Net, K- En Yakın Komşu, Random Forest olarak değiştirilmiştir. Apply Model operatörü ile örnek veri kümesine modelin uygulanması sağlanmaktadır. Performance operatörü ile model performansına ilişkin parametreler belirlenmiştir. Parametreler belirlenirken modelin daha iyi performans göstermesine özen gösterilir. Bu bağlamda yapay sinir ağları için parametreler, öğrenme oranı 0.01, momentum katsayısı 0.9 ve iterasyon sayısı 1000 olarak belirlenmiştir. Destek Vektör Makineleri için kernel/çekirdek tipi dot, kernel önbelleği 200, iterasyon sayısı 100000'dir. K-En Yakın Algoritma için k değeri 10, ölçü türü karışık ölçü ve karışık Öklid uzaklığı seçilmiştir. Rastgele Orman için ağ sayısı 100, kriter en küçük kareler, maksimum derinlik 10 olarak belirlenmiştir.

3.7. Veri Toplama Araçları

Araştırmada Bilgi Güvenliği Ölçeği (Gerçeker, 2012), Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği (Keser & Güldüren, 2015), Bilgi Paylaşım Ölçeği (Aslan, 2014) ve standardizasyon işlemleri araştırmacılar tarafından gerçekleştirilen Örgütsel İletişim Envanteri (Tuna, 2008) ve Kişisel Bilgi formu kullanılmıştır.

Kişisel Bilgi Formu: Örnekleme dahil edilen akademik ve idari personel hakkında cinsiyet, yaş, görev türü, hizmet süresi, görev yapılan akademik veya idari birim, eğitim düzeyi, bilgisayarı/İnterneti kullanma düzeyi, günlük bilgisayar/İnternet kullanma süresi, bilgisayarı/İnterneti kullanma yılı, İnterneti kullanma amacı, sosyal ağ sitelerini kullanma düzeyi, İnternet/sosyal sitelerinde paylaşılan bilgi türü, İnternet/sosyal sitelerinde gizlilik/güvenlik ayarı kontrol sıklığı, İnternet ortamının güvenliğine ilişkin görüşler gibi bilgileri tespit etmeyi sağlayan araştırmacılar tarafından geliştirilen formdur.

Bilgi Güvenliği Ölçeği: Bilgi Güvenliği Ölçeği kuruluşlardaki bilgi güvenliği düzeyini belirlemek amacıyla Gerçeker (2012) tarafından geliştirilmiştir. Ölçek 26 maddeden ve beş alt boyuttan oluşmaktadır. Ölçeğin alt boyutları bilgi güvenliği kültürü, bilgi güvenliği yönetimi, bilgi güvenliği yaklaşımı, bilgi güvenliği uygulaması, bilgi güvenliğinde gizlilik şeklindedir. Ölçek beşli likert tipindedir (1-Tamamen Katılmıyorum /5-Tamamen Katılıyorum) ve ölçeğin Cronbach Alpha güvenirlik katsayısı 0.94 olarak hesaplanmıştır. Bu tez çalışması için hesaplanan Cronbach Alpha güvenirlik katsayısı ise 0.96'dır. Ölçme aracının yapı geçerliliğini sağlamak için bu çalışmada elde edilen veriler üzerinden Açımlayıcı Faktör Analizi (AFA) ve Doğrulayıcı Faktör Analizi (DFA) gerçekleştirilmiştir. AFA sonucunda, faktör yük değerleri Bilgi Güvenliği Kültürü boyutu için 0.632-0.773 aralığında, Bilgi Güvenliği Uygulaması boyutu için 0.527-0.761 aralığında, Bilgi Güvenliği Yaklaşımı boyutu için 0.572-0.732 aralığında, Bilgi Güvenliği Yönetimi boyutu için 0.568-0.754 aralığında, Bilgi Güvenliğinde Gizlilik boyutu için 0.736- 0.831 aralığında değişim gösterdiği belirlenmiştir.

DFA sonucunda uyum değerleri χ^2/sd=2.911; SRMR =0.043, TLI=0.932, CFI =0.938, RMSEA= 0.058 olarak belirlenmiştir. Uyum indekslerinin iyileştirilmesi için uzman görüşü alınarak iki modifikasyon gerçekleştirilmiştir. 1. ve 2. maddeler ile 7. ve 8. maddeler üzerinden modifikasyon gerçekleştirilmiştir. Modifikasyon işlemlerinden sonra DFA sonucunda uyum değerleri χ^2/sd=2.441; SRMR =0.040, TLI=0.948, CFI =0.954, RMSEA= 0.050 olarak belirlenmiştir. Ayrıca Doğrulayıcı Faktör Analizi sonucunda faktör yük değerleri 0.516- 0.752

aralığında değişmektedir. Gerçekleştirilen analizler sonucunda ölçeğin kullanışlı olduğu belirlenmiştir.

Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği: Keser ve Güldüren (2015) tarafından geliştirilen Bilgi Güvenliği Farkındalık Ölçeği, kişisel bilgi güvenliği farkındalık düzeyini belirlemek amacıyla geliştirilmiştir ve 34 maddeden oluşmaktadır. Ölçeğin, "Saldırı ve Tehditler" ile "Kişisel Verilerin Korunması" olarak adlandırılan iki alt boyutu bulunmaktadır. Ölçeğin geçerlik ve güvenirlik çalışması yükseköğretim kurumlarında görev yapan 363 öğretim elamanıyla gerçekleştirilmiştir. Ölçek beşli likert tipindedir (1-Kesinlikle Katılmıyorum /5-Kesinlikle Katılıyorum) ve ölçeğin tamamı için hesaplanan Cronbach Alpha güvenirlik katsayısı 0.97'dir. Bu tez çalışması için hesaplanan Cronbach Alpha güvenirlik katsayısı 0.98 şeklindedir.

Ölçme aracının yapı geçerliliğini sağlamak için bu çalışmada elde edilen veriler üzerinden AFA ve DFA gerçekleştirilmiştir. AFA sonucunda, faktör yük değerleri Saldırı ve Tehditler boyutu için 0.711-0.861aralığında, Kişisel Verilerin Korunması boyutu için 0.638-0.803 aralığında değişim gösterdiği belirlenmiştir. DFA sonucunda uyum değerleri χ^2/sd=5.399; SRMR =0.052, TLI=0.852, CFI =0.861, RMSEA= 0.092 olarak belirlenmiştir. Analiz sonucunda elde edilen uyum indekslerinin yeterli düzeyde olmaması nedeniyle modifikasyon önerileri incelenmiştir. YEM'de model modifikasyonu gerçekleştirilirken modifikasyon indeks değeri en büyük olandan başlanarak sırayla modifikasyonlar gerçekleştirilip her modifikasyon sonrası model yeniden test edilmiştir (Şen, 2020: 35). Uyum indekslerinin iyileştirilmesi için dört modifikasyon gerçekleştirilmiştir. Modifikasyon önerileri dikkate alınarak "Saldırı ve Tehditler" alt boyutunda yer alan 15. ve 16. maddeler ile 1. ve 2. maddeler arasında; "Kişisel Verilerin Korunması" alt boyutunda yer alan 30. ve 31. maddeler ile 17. ve 18. maddeler arasında uzman görüşü alınarak modifikasyon yapılmasına karar verilmiştir.

Modifikasyon gerçekleştirildikten sonra yapılan DFA sonucunda uyum değerleri χ^2/sd=4.203; SRMR =0.051, TLI=0.892, CFI =0.900, RMSEA= 0.078 olarak belirlenmiştir. Analiz sonucunda elde edilen değerler, eşik değerler ile karşılaştırıldığında TLI değerinin eşik değerinin biraz altında olduğu belirlenmiştir. Bu TLI değeri iyi uyuma sahip olmadığını gösterirken diğer uyum indekslerinin eşik değerler içerisinde olduğu görülmektedir. Bu sonuç modelin iyi uyum gösterdiğini işaret etmektedir (Şen, 2020). Ayrıca DFA sonucunda faktör yük değerleri 0.531-0.693 aralığında değişmektedir. Gerçekleştirilen analizler sonucunda ölçeğin kullanışlı olduğu belirlenmiştir.

Bilgi Paylaşımı Ölçeği: Wang ve Wang (2012) tarafından geliştirilen ölçeğin, Türkçe uyarlaması Aslan (2014), tarafından gerçekleştirilmiştir. Ölçek bilgi paylaşımı, inovasyon, firma performansı olmak üzere üç temel bileşenden ve 33 maddeden oluşmaktadır. Bilgi paylaşımı temel bileşeni, beşli likert tipinde (1-Kesinlikle Katılmıyorum /5-Kesinlikle Katılıyorum) olup 11 maddeden ve iki alt boyuttan oluşmaktadır. Ölçeğin Açık Bilgi Paylaşımı alt boyutu için hesaplanan Cronbach Alpha güvenirlik katsayısı 0.81 ve Örtük Bilgi Paylaşımı alt boyutu için hesaplanan Cronbach Alpha güvenirlik katsayısı 0.89'dur. Bu tez çalışması için hesaplanan Cronbach Alpha güvenirlik katsayısı ise 0.910 şeklindedir.

Ölçme aracının yapı geçerliliğini sağlamak için bu çalışmada elde edilen veriler üzerinden AFA ve DFA gerçekleştirilmiştir. AFA sonucunda, faktör yük değerleri Açık Bilgi Paylaşım boyutu için 0.638- 0.851 aralığında, Örtük Bilgi Paylaşım boyutu için ise 0.660 -0.750 aralığında değişim gösterdiği belirlenmiştir. DFA sonucunda uyum değerleri χ^2/sd=7,55; SRMR =0.050, TLI=0.928, CFI =0.908, RMSEA= 0.105 olarak belirlenmiştir.

Uyum indekslerinin iyileştirilmesi için bir modifikasyon gerçekleştirilmiştir. Uzman görüşü alınarak Örtük Bilgi Paylaşımı alt boyutunda yer alan 7. ve 8. maddeler birleştirilmiştir. Modifikasyon gerçekleştirildikten sonra yapılan DFA sonucunda uyum değerleri χ^2/sd=5; SRMR =0.044, TLI=0.928, CFI =0.945, RMSEA= 0.080 olarak belirlenmiştir. DFA sonucunda faktör yük değerleri 0.426- 0.698 aralığında değişmektedir. Gerçekleştirilen analizler sonucunda ölçeğin kullanışlı olduğu belirlenmiştir.

Örgütsel İletişim Envanteri: Tuna (2008), tarafından geliştirilen Örgütsel İletişim Envanteri 20 maddeden oluşmaktadır. Geliştirilen envanterin amacı, örgütteki iletişim ile ilgili görüş elde edebilmektedir. Envanter beşli likert tipindedir (Asla=1, nadiren=2, bazen=3, sık sık=4, sürekli olarak=5) ve envanterin tamamı için hesaplanan Cronbach Alpha güvenirlik katsayısı 0.85'tir. Envanterde yer alan yedinci ifade olumsuzdur, bu nedenle ters puanlanmış ve kodlanmıştır. Örgütsel İletişim Envanterinin istatistiksel analizlerinin yapılabilmesi için standardizasyon işlemlerinin gerçekleştirilmesine ihtiyaç duyulmuştur.

Örgütsel İletişim Envanterinin Standardizasyon İşlemleri

Envanterin standardizasyonu gerçekleştirmek için AFA ve DFA gerçekleştirilmiştir. AFA çalışmasının örneklemini Türkiye'nin güneydoğusunda yer alan bir üniversitede görev yapan seçkisiz örneklem yöntemi ile belirlenmiş 136 akademik ve idari personel oluşturmaktadır. DFA çalışmasının örneklemini ise Türkiye'nin doğusunda yer alan bir üniversitede görev yapan seçkisiz örneklem yöntemi ile belirlenmiş 146 akademik ve idari personel oluşturmaktadır. Kline (1994: 22), ölçek geliştirmek için örneklemin madde sayısının beş katı olmasının yeterli olduğunu belirtmiştir. Envanter çevrimiçi olarak çalışma grubuna uygulanmıştır.

Verilerin ve örneklemin faktör analizine uygunluğunun belirlenmesi amacıyla Kaiser-Meyer-Olkin (KMO) ve Bartlett Küresellik testi gerçekleştirilmiştir. Analiz sonucunda KMO değeri 0.878 ve Bartlett Küresellik testi sonucu 0.000 ($p<0.005$) olduğu belirlenmiştir. Faktör analizinin gerçekleştirilebilmesi için KMO değerinin 0.60'dan büyük olması ve Bartlett's testinin $p<0.05$ olması beklenmektedir (Tabachnick ve Fidel, 2007: 614).

Elde edilen değerler, verilerin faktör analizine uygun olduğunu göstermektedir. AFA'da envanterde yer alan 20 madde ile başlanmıştır ve öz değeri 1'den büyük iki alt boyut tespit edilmiştir. Belirlenen iki alt boyut toplam varyansın %48.412'sini açıklamaktadır. Birden fazla alt boyutta yüksek yük değerine sahip ve matrix değeri farkının 0.10'dan az olan dört madde (madde 7, madde 9, madde 18, madde 20) sırasıyla envanterden çıkartılmıştır. Her madde çıkarımından sonra faktör analizi tekrarlanmıştır. Analizler sonucunda, madde yükü alt kesme noktası 0.40 ve üzeri 16 madde öz değeri 1'den büyük iki alt boyut altında toplanmıştır ve bu iki alt boyut ölçeğe ilişkin açıkladığı varyans %58.419'dur.

Döndürme işlemi, faktörler ve değişkenler arasındaki yüksek korelasyonları en üst düzeye çıkarmak, düşük olanları da en aza indirmek için kullanılır. Çok sayıda döndürme yöntemi mevcuttur ancak yaygın olarak varimax yöntemi kullanılmaktadır. Varimax yöntemi, her faktör için yüksek yük değerlerini daha yüksek ve düşük yük değerlerini daha düşük yaparak faktör yüklerinin varyansını en yüksek düzeye çıkarmak için kullanılır (Tabachnick ve Fidel, 2007: 620). Varimax yöntemi ile yapılan döndürme işlemi sonucunda ölçeğin alt boyutlarında yer alan maddeler belirlenmiştir. Madde yük değerleri ve yer aldıkları alt boyutlar Tablo 7'de gösterilmiştir.

Tablo 7. Madde Yük Değerleri

Madde	Faktör Yükü	Ortalama	SS	Madde-toplam Korelasyonu
1.Faktör (Formel İletişim)	**Açıklanan Varyans : 45.054**			
m14	.829	3.559	.7960	.732
m5	.821	3.610	.7904	.687
m3	.812	3.507	.7698	.653
m8	.792	3.735	.8712	.676
m4	.785	3.596	.7924	.694
m17	.779	3.478	.8774	.679
m2	.774	3.537	.7785	.661
m10	.749	3.603	.8099	.673
m1	.745	3.713	.8336	.603
m11	.734	3.529	.7297	.645
m15	.728	3.522	.8252	.650
m19	.690	3.662	.7815	.648
2. Faktör (İnformel İletişim)	**Açıklanan Varyans : 13.365**			
m13	.806	3.213	.6135	.673
m12	.714	3.397	.7022	.650
m6	.682	3.243	.5900	.675
m16	.588	2.912	.6608	.645

Tablo 7 incelendiğinde madde yük değerlerinin 0.588 ile 0.829 arasında olduğu belirlenmiştir. Madde yük değerlerinin 0.3 veya daha büyük yüklemeler önemli olarak kabul edilmektedir (Kline, 1994: 52). Bu çalışmada elde edilen madde yük değerlerinin önemli olduğu görülmektedir. Uzman görüşü alınarak ölçeğin alt boyutları Formel İletişim ve İnformel İletişim olarak isimlendirilmiştir.

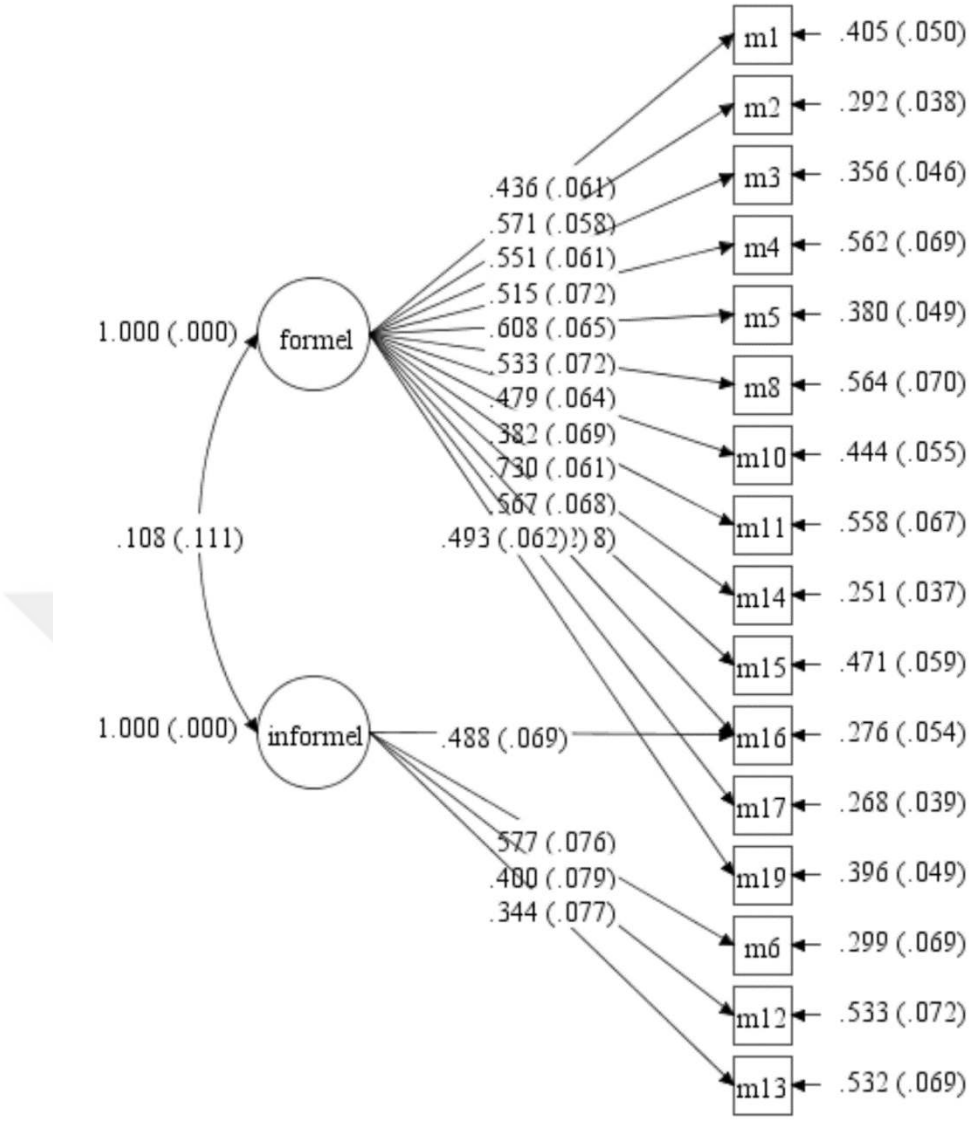
Tablo 8. Faktörlerin Açıkladıkları Toplam Varyans Ve Özdeğerleri

Faktörler	Faktör Öz değerleri	Açıklanan Faktör Varyansı %	Açıklanan Toplam Varyans %
Formel İletişim	7.209	45.054	45.054
İnformel İletişim	2.138	13.365	58.419

Örgütsel İletişim ölçeği iki alt boyutludur ve bu iki alt boyutun açıkladığı toplam varyans %58.419'dur.

Doğrulayıcı Faktör Analizi

AFA sonucunda ortaya çıkan iki alt boyutlu modelin yapı geçerliliğini değerlendirmek amacıyla DFA gerçekleştirilmiştir. Analiz sonucunda χ^2/sd (154.85/103, p=0.00) RMSEA =0.059, NFI=0.92, NNFI= 0.97, CFI=0.97, RFI=0.91 AGFI=0.84 GFI=0.88 RMR =0.048 ve bu değerlerin iyi uyum gösterdiği belirlenmiştir (Harrington, 2009: 29; Kline, 1994: 97-98).



Şekil 5. DFA Sonucu Madde Yük Değerleri

Güvenirlik İşlemleri

Ölçeğin tamamı için hesaplanan Cronbasch's Alpha katsayısı 0.902'dir. Ölçeğin Formel İletişim alt boyutuna yönelik hesaplanan Cronbasch's Alpha katsayısı 0.938; İnformel İletişim alt boyutuna yönelik hesaplanan Cronbasch's Alpha katsayısı ise 0.876 olarak belirlenmiştir.

Örgütsel İletişim Envanteri (Tuna, 2008) standardizasyon işlemlerinden sonra Örgütsel İletişim Ölçeği olarak ifade edilmiştir. Örgütsel İletişim ölçeğinin yapı geçerliliğini sağlamak için bu çalışmada elde edilen veriler üzerinden AFA ve DFA gerçekleştirilmiştir. AFA sonucunda, faktör yük değerleri Formel İletişim boyutu için 0.597- 0.752 aralığında, İnformel İletişim boyutu için ise 0.512-0.748 aralığında değişim gösterdiği belirlenmiştir. DFA sonucunda uyum değerleri χ^2/sd=3.51; SRMR =0.054, TLI=0.890, CFI =0.905, RMSEA= 0.065 olarak belirlenmiştir. Uyum indekslerinin iyileştirilmesi için bir modifikasyon gerçekleştirilmiştir. İnformel iletişim alt boyutunda yer alan 2. ve 3. maddeler uzman görüşü alınarak birleştirilmiştir. Modifikasyon gerçekleştirildikten sonra yapılan DFA sonucunda uyum değerleri χ^2/sd=2.81; SRMR =0.051, TLI=0.920, CFI =0.932, RMSEA= 0.053 olarak belirlenmiştir. DFA sonucunda faktör yük

değerleri 0.414- 0.667 aralığında değişmektedir. Gerçekleştirilen analizler sonucunda ölçeğin kullanışlı olduğu belirlenmiştir.

3.8. Tez Çalışmasının Geçerlik ve Güvenirliği

Bu çalışmada araştırmada kullanılan ölçekler ve araştırma sürecine yönelik ilgili alan yazında yer alan bilgiler ışığında geçerlik ve güvenirlik çalışmaları gerçekleştirilmiştir. Ayrıca geçerlik ve güvenirliği sağlamak amacıyla araştırma sürecinde bazı önlemler alınmıştır. Gerçekleştirilen çalışmalar ve önlemler maddeler halinde sunulmuştur.

Geçerlik Önlemleri

- Araştırma yönteminin detaylı tanıtılması (Büyüköztürk vd., 2012: 276)
- Araştırma evrenin ve örnekleminin özelliklerinin açıklanması (Büyüköztürk vd., 2012: 276; McMillan ve Schumacher, 2014: 37)
- Veri analiz sürecinin detaylı bir şekilde açıklanması (Hedges, 2019: 47)
- Veri toplama araçlarının ve veri toplama sürecinin açıklanması (McMillan ve Schumacher, 2014: 187)
- Katılımcıların gönüllü bir biçimde araştırmaya katılması (McMillan ve Schumacher, 2014: 130)
- Çalışmanın varsayımların (sayıltıların) ve sınırlılıkların belirlenmesi (McMillan ve Schumacher, 2014: 23,163)
- Araştırma sürecinin açıklanması (Harris, Hedges ve Valentine, 2019: 11)
- Araştırmacının rolünün açıklanması (Harris, Hedges ve Valentine, 2019: 33)

Güvenirlik Önlemleri

- Araştırma amacına uygun olarak ilgili literatürün incelenmesi, tartışılması ve sentezlenmesi (Harris, Hedges ve Valentine, 2019: 5)
- Ölçme formundan elde edilen verilerin araştırmacı dışında kontrol edilmesi (Cohen, Manion ve Morrison, 2005: 173)
- Araştırma sürecinde uzman görüşünün alınması (Harris, Hedges ve Valentine, 2019: 311)

4. BULGULAR

Bu bölümde, araştırmadan elde edilen bulgular ve bu bulgulara yönelik yorumlara yer verilmiştir.

4.1. Kurumsal Bilgi Güvenliği, Bilgi Güvenliği Farkındalığı, Örgütsel İletişim ve Örgütsel Bilgi Paylaşımı Değişkenlerine ait Ortalama ve Standart Sapma Değerleri

Bu bölümde araştırmaya katılan akademik ve idari personelin kurumsal bilgi güvenliği, bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı değişkenlerine ilişkin algılarına yönelik bulgulara yer verilmiştir. Araştırmada kullanılan değişkenlere ait ortalamalar ve standart sapma değerleri Tablo 9'da sunulmuştur.

Tablo 9. Akademik ve İdari Personelin Araştırma Kapsamındaki Değişkenlere İlişkin Algıları

Değişken	N	$\overline{X}$	SS	Puan Aralığı
Kurumsal Bilgi Güvenliği	479	3.45	.540	Yüksek
Kurumsal Bilgi Güvenliği Ölçeği Alt Boyutları				
Bilgi Güvenliği Kültürü Boyutu	479	3.41	.707	Yüksek
Bilgi Güvenliği Uygulaması Boyutu	479	3.32	.607	Orta
Bilgi Güvenliği Yaklaşımı Boyutu	479	3.41	.662	Yüksek
Bilgi Güvenliği Yönetimi Boyutu	479	3.44	.606	Yüksek
Bilgi Güvenliğinde Gizlilik Boyutu	479	3.86	.699	Yüksek
Bilgi Güvenliği Farkındalığı Düzeyi Belirleme	479	3.54	.579	Yüksek
Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği Alt Boyutları				
Saldırı ve Tehditler Boyutu	479	3.26	.656	Orta
Kişisel Verilerin Korunması Boyutu	479	3.78	.606	Yüksek
Örgütsel İletişim	479	3.48	.623	Yüksek
Örgütsel İletişim Ölçeği Alt Boyutları				
Formel İletişim Boyutu	479	3.48	.623	Yüksek
İnformel İletişim Boyutu	479	2.90	.569	Orta
Bilgi Paylaşımı	479	3.42	.556	Yüksek
Bilgi Paylaşım Ölçeği Alt Boyutları				
Açık Bilgi Paylaşımı Boyutu	479	3.32	.673	Orta
Örtük Bilgi Paylaşımı Boyutu	479	3.47	.590	Yüksek

Tablo 9'da yer alan ortalama ve puan aralıkları incelendiğinde, akademik ve idari personelin kurumsal bilgi güvenliği ($\overline{X}$=3.45), bilgi güvenliği farkındalığı ($\overline{X}$=3.54), örgütsel iletişim ($\overline{X}$=3.48) ve bilgi paylaşımı ($\overline{X}$=3.42) düzeylerinin yüksek olduğu görülmektedir. Araştırmada kullanılan ölçeklerin alt boyutlarına yönelik ortalama ve puan aralıkları incelendiğinde, kurumsal bilgi güvenliğinin bilgi güvenliği kültürü ($\overline{X}$=3.41), bilgi güvenliği yaklaşımı ($\overline{X}$=3.41), bilgi güvenliği yönetimi ($\overline{X}$=3.44), bilgi güvenliğinde gizlilik ($\overline{X}$=3.86) alt boyutlarının yüksek düzey, bilgi güvenliği uygulaması ($\overline{X}$=3.32) alt boyutunun ise orta düzey olduğu belirlenmiştir.

Kişisel bilgi güvenliği farkındalığının saldırı ve tehditler ($\overline{X}$=3.26) alt boyutunun orta düzey, kişisel verilerin korunması ($\overline{X}$=3.78) alt boyutunun ise yüksek olduğu sonucuna ulaşılmıştır.

Örgütsel iletişim ölçeğinin alt boyutlarına ilişkin ortalama ve puan aralıkları incelendiğinde, formel iletişim alt boyutunun yüksek ($\overline{X}$=3.48), informel iletişim ($\overline{X}$=2.90) alt boyutunun ise orta düzey olduğu belirlenmiştir.

Bilgi paylaşım ölçeğinin alt boyutlarına ilişkin ortalama ve puan aralıkları incelendiğinde açık bilgi paylaşımı ($\overline{X}$=3.32) alt boyutunun orta, örtük bilgi paylaşımı ($\overline{X}$=3.47) alt boyutunun yüksek düzey olduğu görülmektedir.

4.2. Kurumsal Bilgi Güvenliği, Bilgi Güvenliği Farkındalığı, Örgütsel İletişim ve Örgütsel Bilgi Paylaşımı Değişkenlerinin Demografik Bilgilere Göre Farklılık Analizi Sonuçları

Bu bölümde katılımcıların kurumsal bilgi güvenliği, bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı değişkenlerinin demografik bilgilere göre farklılık analizi sonuçları yer almaktadır. Analiz sonuçlarına göre katılımcıların kurumsal bilgi güvenliği, bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı, İnternette gezinirken/sosyal ağ sitelerinde kişisel bilgilerini doğru olarak verme, İnternet ortamlarının güvenli olduğunu düşünme, İnternet ortamlarında paylaştığınız bilgilerin başkaları tarafından alınıp kullanılabileceğini düşünme durumuna göre anlamlı farklılık göstermemektedir.

4.2.1. Araştırma Değişkenlerinin Cinsiyete Göre Farklılık Analizi Sonuçları

Katılımcıların kurumsal bilgi güvenliği, bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı değişkenlerinin cinsiyet değişkenine göre farklılık analizi sonuçları bu başlık altında yer almaktadır.

Tablo 10. Katılımcıların Görüşlerinin Cinsiyet Değişkenine Göre Karşılaştırılması

Değişken	Cinsiyet	N	$\overline{X}$	SS	t	p
Kurumsal Bilgi Güvenliği	Erkek	175	3.46	.548	0.211	0.833
	Kadın	304	3.45	.537		
Kurumsal Bilgi Güvenliği Ölçeği Alt Boyutları						
Bilgi Güvenliği Kültürü Boyutu	Erkek	175	3.41	.693	0.086	0.931
	Kadın	304	3.41	.717		
Bilgi Güvenliği Uygulaması Boyutu	Erkek	175	3.32	.632	0.125	0.901
	Kadın	304	3.33	.593		
Bilgi Güvenliği Yaklaşımı Boyutu	Erkek	175	3.41	.671	0.202	0.840
	Kadın	304	3.42	.657		
Bilgi Güvenliği Yönetimi Boyutu	Erkek	175	3.45	.606	0.392	0.695
	Kadın	304	3.43	.607		
Bilgi Güvenliğinde Gizlilik Boyutu	Erkek	175	3.90	.699	0.832	0.406
	Kadın	304	3.84	.700		
Bilgi Güvenliği Farkındalığı	Erkek	175	3.50	.521	0.994	0.321
	Kadın	304	3.56	.610		
Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği Alt Boyutları						
Saldırı ve Tehditler Boyutu	Erkek	175	3.22	.594	1.155	0.249
	Kadın	304	3.29	.688		
Kişisel Verilerin Korunması Boyutu	Erkek	175	3.75	.557	0.683	0.495
	Kadın	304	3.79	.633		
Örgütsel İletişim	Erkek	175	3.51	.603	0.801	0.424
	Kadın	304	3.46	.635		
Örgütsel İletişim Ölçeği Alt Boyutları						
Formel İletişim Boyutu	Erkek	175	3.51	.603	0.801	0.424
	Kadın	304	3.46	.635		
İnformel İletişim Boyutu	Erkek	175	2.84	.549	1.859	0.064
	Kadın	304	2.94	.578		
Bilgi Paylaşımı	Erkek	175	3.43	.589	0.501	0.617
	Kadın	304	3.41	.536		
Bilgi Paylaşım Ölçeği Alt Boyutları						
Açık Bilgi Paylaşımı Boyutu	Erkek	175	3.36	.692	0.875	0.382
	Kadın	304	3.30	.662		
Örtük Bilgi Paylaşımı Boyutu	Erkek	175	3.48	.620	0.171	0.864
	Kadın	304	3.47	.573		

Tablo 10 incelendiğinde, çalışmada kullanılan değişkenlerin cinsiyete göre anlamlı farklılık göstermediği belirlenmiştir.

4.2.2. Araştırma Değişkenlerinin Yaş Göre Farklılık Analizi Sonuçları

Bu başlık altında katılımcıların kurumsal bilgi güvenliği, bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı değişkenlerinin yaş değişkenine göre farklılık analizi sonuçları yer almaktadır.

Tablo 11. Katılımcıların Görüşlerinin Yaş Değişkenine Göre Karşılaştırılması

Değişken	Yaş	N	$\bar{X}$	SS	F	p	Fark	η2
Kurumsal Bilgi Güvenliği	A. 35 yaş altı	121	3.54	.596	1.723		-	
	B.30-44	152	3.45	.543				
	C.45-55	139	3.41	.517				
	D.55 ve üzeri	67	3.38	.460				
Kurumsal Bilgi Güvenliği Ölçeği Alt Boyutları								
Bilgi Güvenliği Kültürü Boyutu	A. 35 yaş altı	152	3.40	.570	0.870	0.456	-	
	B.30-44	139	3.36	.479				
	C.45-55	67	3.29	.488				
	D.55 ve üzeri	479	3.42	.556				
Bilgi Güvenliği Uygulaması Boyutu	A. 35 yaş altı	121	3.49	.726	0.825	0.480	-	
	B.30-44	152	3.41	.679				
	C.45-55	139	3.38	.721				
	D.55 ve üzeri	67	3.33	.711				
Bilgi Güvenliği Yaklaşımı Boyutu	A. 35 yaş altı	479	3.41	.707	1.094	0.351	-	
	B.30-44	121	3.39	.695				
	C.45-55	152	3.31	.561				
	D.55 ve üzeri	139	3.30	.612				
Bilgi Güvenliği Yönetimi Boyutu	A. 35 yaş altı	67	3.26	.523	1.993	0.114	-	
	B.30-44	479	3.32	.607				
	C.45-55	121	3.50	.704				
	D.55 ve üzeri	152	3.40	.646				
Bilgi Güvenliğinde Gizlilik Boyutu	A. 35 yaş altı	139	3.39	.671	1.879	0.132	-	
	B.30-44	67	3.35	.595				
	C.45-55	479	3.41	.662				
	D.55 ve üzeri	121	3.53	.658				
Bilgi Güvenliği Farkındalığı	A. 35 yaş altı	479	3.45	.540	3.797	0.010	A>C A>D	.023
	B.30-44	121	3.67	.642				
	C.45-55	152	3.55	.602				
	D.55 ve üzeri	139	3.46	.544				
Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği Alt Boyutları								
Saldırı ve Tehditler Boyutu	A. 35 yaş altı	152	3.47	.637	3.235	0.022	A>C	.020
	B.30-44	139	3.37	.561				
	C.45-55	67	3.36	.506				
	D.55 ve üzeri	479	3.44	.606				

Kişisel Verilerin Korunması Boyutu	A. 35 yaş altı	121	3.99	.622	3.273	0.021	A>B A>C	.020
	B.30-44	152	3.84	.707				
	C.45-55	139	3.82	.735				
	D.55 ve üzeri	67	3.78	.724				
Örgütsel İletişim	A. 35 yaş altı	67	3.42	.413	2.132	0.095	-	
	B.30-44	479	3.54	.579				
	C.45-55	121	3.58	.667				
	D.55 ve üzeri	152	3.49	.643				
Örgütsel İletişim Ölçeği Alt Boyutları								
Formel İletişim Boyutu	A. 35 yaş altı	479	3.86	.699	2.132	0.095		
	B.30-44	121	3.39	.708				
	C.45-55	152	3.29	.653				
	D.55 ve üzeri	139	3.17	.639				
İnformel İletişim Boyutu	A. 35 yaş altı	67	3.15	.557	3.519	0.015	A>C	.021
	B.30-44	479	3.26	.656				
	C.45-55	121	3.91	.663				
	D.55 ve üzeri	152	3.78	.647				
Bilgi Paylaşımı	A. 35 yaş altı	139	3.41	.566	5.349	0.001	A>B A>C A>D	.032
	B.30-44	67	3.38	.593				
	C.45-55	479	3.48	.623				
	D.55 ve üzeri	121	3.58	.621				
Bilgi Paylaşım Ölçeği Alt Boyutları								
Açık Bilgi Paylaşımı Boyutu	A. 35 yaş altı	139	3.72	.570	4.988	0.002	A>C A>D	.030
	B.30-44	67	3.66	.414				
	C.45-55	479	3.78	.606				
	D.55 ve üzeri	121	3.58	.667				
Örtük Bilgi Paylaşımı Boyutu	A. 35 yaş altı	152	3.49	.643	4.215	0.006	A>D	.025
	B.30-44	139	3.41	.566				
	C.45-55	67	3.38	.593				
	D.55 ve üzeri	479	3.48	.623				

Tablo 11 incelendiğinde, kurumsal bilgi güvenliği ve alt boyutlarının, örgütsel iletişim ve formel iletişim alt boyutunun yaş değişkenine göre anlamlı farklılık olmadığı ancak bilgi güvenliği farkındalığı, bilgi paylaşımı, saldırı ve tehditler boyutu, kişisel verilerin korunması, informel iletişim, açık bilgi paylaşımı, örtük bilgi paylaşımı boyutlarının yaş değişkeni açısından anlamlı farklılık olduğu görülmektedir. Grupların homojen dağılması nedeniyle farklılığın hangi yaş grupları arasında olduğunu belirlemek amacıyla post-hoc analizlerinden Scheffe testi yapılmıştır. Ayrıca yaş değişkeninin etki düzeyini belirlemek için eta kare (η2) değeri hesaplanmıştır.

Bilgi Güvenliği Farkındalığı yaş değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın 35 yaş altı ve 30-44 yaş ile 35 yaş altı ve 45-55 yaş aralığında olan katılımcılar arasında olduğu belirlenmiştir ve bu fark 35 yaş altı olan katılımcıların lehinedir. Etki değerini

belirlemek için hesaplanan eta kare değerinin .023 olduğu belirlenmiştir ve bu sonuç yaş değişkeninin bilgi güvenliği farkındalığı üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Bilgi güvenliği farkındalığı ölçeğinin saldırı ve tehditler boyutu yaş değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın 35 yaş altı ve 45-55 yaş aralığında olan katılımcılar arasında olduğu belirlenmiştir ve bu fark 35 yaş altı olan katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .020 olduğu belirlenmiştir. Bu sonuç yaş değişkeninin üniversitede görev yapan akademik ve idari personelin saldırı ve tehditler farkındalığı üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Bilgi güvenliği farkındalığı ölçeğinin kişisel verilerin korunması alt boyutu yaş değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın 35 yaş altı ve 30-44 yaş ile 35 yaş altı ve 45-55 yaş aralığında olan katılımcılar arasında olduğu belirlenmiştir ve bu fark 35 yaş altı olan katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .020 olduğu bulgulanmıştır. Bu sonuca göre yaş değişkeninin üniversitede görev yapan akademik ve idari personelin kişisel verilerin korunması üzerinde orta büyüklükte etkiye sahip olduğu belirlenmiştir.

Örgütsel iletişim ölçeğinin informel iletişim boyutu yaş değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın 35 yaş altı ve 45-55 yaş aralığında olan katılımcılar arasında olduğu belirlenmiştir ve bu fark 35 yaş altı olan katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .021 olduğu belirlenmiştir. Bu sonuç yaş değişkeninin üniversitede görev yapan akademik ve idari personelin informel iletişimi üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Bilgi paylaşımı yaş değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın 35 yaş altı ve 45-55 yaş ile 35 yaş altı ve 55 yaş ve üzeri olan katılımcılar arasında olduğu ve bu farkın 35 yaş altı olan katılımcıların lehine olduğu belirlenmiştir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .032 olduğu belirlenmiştir. Bu sonuç yaş değişkeninin üniversitede görev yapan akademik ve idari personelin bilgi paylaşımları üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Açık bilgi paylaşım boyutu yaş değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın 35 yaş altı ve 45-55 yaş ile 35 yaş altı ve 55 yaş ve üzeri aralığında olan katılımcılar arasında olduğu belirlenmiştir ve bu fark 35 yaş altı olan katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .030 olduğu belirlenmiştir. Bu sonuç yaş değişkeninin üniversitede görev yapan akademik ve idari personelin açık bilgi paylaşımları üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Örtük bilgi paylaşımı boyutu yaş değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın 35 yaş altı ile 55 yaş ve üzeri olan katılımcılar arasında olduğu ve bu farkın 35 yaş altı olan katılımcıların lehine olduğu belirlenmiştir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .025 olduğu belirlenmiştir. Bu sonuç yaş değişkeninin üniversitede görev yapan akademik ve idari personelin örtük bilgi paylaşımları üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

4.2.3. Araştırma Değişkenlerinin Hizmet Süresine Göre Farklılık Analizi Sonuçları

Bu başlık altında katılımcıların kurumsal bilgi güvenliği, bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı değişkenlerinin hizmet süresi değişkenine göre farklılık analizi sonuçları yer almaktadır.

Tablo 12. Katılımcıların Görüşlerinin Hizmet Süresi Değişkenine Göre Karşılaştırılması

Değişken	Hizmet Süresi	N	$\bar{X}$	SS	F	p	Fark	η2
Kurumsal Bilgi Güvenliği	A.5 yıldan az	67	3.59	.591	2.017	0.091		
	B.5-10 yıl	97	3.46	.533				
	C. 11-20 yıl	109	3.36	.578				
	D.21-30 yıl	129	3.48	.505				
	E.30 yıl ve üzeri	77	3.41	.490				
Kurumsal Bilgi Güvenliği Ölçeği Alt Boyutları								
Bilgi Güvenliği Kültürü Boyutu	A.5 yıldan az	67	3.54	.696	1.530	.192		
	B.5-10 yıl	97	3.40	.679				
	C. 11-20 yıl	109	3.29	.757				
	D.21-30 yıl	129	3.47	.668				
	E.30 yıl ve üzeri	77	3.38	.734				
Bilgi Güvenliği Uygulaması Boyutu	A.5 yıldan az	67	3.44	.652	1.530	.192		
	B.5-10 yıl	97	3.32	.614				
	C. 11-20 yıl	109	3.22	.639				
	D.21-30 yıl	129	3.34	.590				
	E.30 yıl ve üzeri	77	3.33	.527				
Bilgi Güvenliği Yaklaşımı Boyutu	A.5 yıldan az	67	3.55	.682	1.334	.256		
	B.5-10 yıl	97	3.43	.626				
	C. 11-20 yıl	109	3.33	.697				
	D.21-30 yıl	129	3.43	.684				
	E.30 yıl ve üzeri	77	3.37	.587				
Bilgi Güvenliği Yönetimi Boyutu	A.5 yıldan az	67	3.58	.691	1.461	.213		
	B.5-10 yıl	97	3.45	.609				
	C. 11-20 yıl	109	3.39	.635				
	D.21-30 yıl	129	3.46	.560				
	E.30 yıl ve üzeri	77	3.36	.548				
Bilgi Güvenliğinde Gizlilik Boyutu	A.5 yıldan az	67	4.01	.574	2.384	.051		
	B.5-10 yıl	97	3.96	.625				
	C. 11-20 yıl	109	3.74	.806				
	D.21-30 yıl	129	3.87	.698				

	E.30 yıl ve üzeri	77	3.77	.701				
Bilgi Güvenliği Farkındalığı	A.5 yıldan az	67	3.72	.618	2.852	0.023	A>E	.023
	B.5-10 yıl	97	3.58	.556				
	C. 11-20 yıl	109	3.48	.631				
	D.21-30 yıl	129	3.52	.561				
	E.30 yıl ve üzeri	77	3.42	.490				
Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği Alt Boyutları								
Saldırı ve Tehditler Boyutu	A.5 yıldan az	67	3.44	.691	2.520	.040	A>E	.020
	B.5-10 yıl	97	3.34	.618				
	C. 11-20 yıl	109	3.21	.681				
	D.21-30 yıl	129	3.23	.661				
	E.30 yıl ve üzeri	77	3.13	.596				
Kişisel Verilerin Korunması Boyutu	A.5 yıldan az	67	3.97	.639	2.504	.042	A>E	.020
	B.5-10 yıl	97	3.79	.586				
	C. 11-20 yıl	109	3.72	.673				
	D.21-30 yıl	129	3.78	.585				
	E.30 yıl ve üzeri	77	3.68	.502				
Örgütsel İletişim	A.5 yıldan az	67	3.67	.609	1.958	0.100		
	B.5-10 yıl	97	3.47	.679				
	C. 11-20 yıl	109	3.42	.645				
	D.21-30 yıl	129	3.46	.563				
	E.30 yıl ve üzeri	77	3.42	.610				
Örgütsel İletişim Ölçeği Alt Boyutları								
Formel İletişim Boyutu	A.5 yıldan az	67	3.67	.609	1.958	.100		
	B.5-10 yıl	97	3.47	.679				
	C. 11-20 yıl	109	3.42	.645				
	D.21-30 yıl	129	3.46	.563				
	E.30 yıl ve üzeri	77	3.42	.610				
İnformel İletişim Boyutu	A.5 yıldan az	67	2.94	.583	4.643	.001	B>C B>D	.037
	B.5-10 yıl	97	3.10	.562				
	C. 11-20 yıl	109	2.82	.585				
	D.21-30 yıl	129	2.82	.555				
	E.30 yıl ve üzeri	77	2.86	.509				
Bilgi Paylaşımı	A.5 yıldan az	67	3.65	.589	4.960	0.001	A>C A>D A>E	.040
	B.5-10 yıl	97	3.49	.586				
	C. 11-20 yıl	109	3.30	.574				
	D.21-30 yıl	129	3.37	.491				
	E.30 yıl ve üzeri	77	3.37	.503				

Bilgi Paylaşım Ölçeği Alt Boyutları								
Açık Bilgi Paylaşımı Boyutu	A.5 yıldan az	67	3.48	.692	2.698	.030	A>C A>D A>E	.022
	B.5-10 yıl	97	3.44	.693				
	C. 11-20 yıl	109	3.25	.674				
	D.21-30 yıl	129	3.23	.637				
	E.30 yıl ve üzeri	77	3.31	.659				
Örtük Bilgi Paylaşımı Boyutu	A.5 yıldan az	67	3.74	.598	5.638	.000	A>C A>D A>E	.045
	B.5-10 yıl	97	3.52	.605				
	C. 11-20 yıl	109	3.34	.628				
	D.21-30 yıl	129	3.45	.551				
	E.30 yıl ve üzeri	77	3.40	.494				

Tablo 12 incelendiğinde, kurumsal bilgi güvenliği ve alt boyutlarının, örgütsel iletişim ve formel iletişim alt boyutunun hizmet süresi değişkenine göre anlamlı farklılık göstermediği, ancak bilgi güvenliği farkındalığı, bilgi paylaşımı, saldırı ve tehditler boyutu, kişisel verilerin korunması, informel iletişim, açık bilgi paylaşımı, örtük bilgi paylaşımı boyutlarının hizmet süresi değişkenine göre anlamlı farklılık gösterdiği belirlenmiştir. Grupların homojen dağılması nedeniyle farklılığın hangi hizmet süresine sahip gruplar arasında olduğunu belirlemek amacıyla post-hoc analizlerinden Scheffe testi yapılmıştır. Ayrıca hizmet süresi değişkeninin etki düzeyini belirlemek için eta kare (η2) değeri hesaplanmıştır.

Bilgi güvenliği farkındalığı hizmet süresine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın 5 yıldan az ve 30 yıl ve üzeri olan katılımcılar arasında ve bu farkın 5 yıldan az hizmet süresine sahip olan katılımcıların lehine olduğu belirlenmiştir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .023 olduğu belirlenmiştir. Bu sonuç hizmet süresi değişkeninin üniversitede görev yapan akademik ve idari personelin bilgi güvenliği farkındalığı üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Bilgi güvenliği farkındalığı ölçeğinin saldırı ve tehditler boyutu ile kişisel verilerin korunması boyutları hizmet süresine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın 5 yıldan az ve 30 yıl ve üzeri olan katılımcılar arasında olduğu belirlenmiştir. Bu fark hizmet süresi 5 yıldan az olan katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare değerinin her iki farkındalık için .020 olduğu belirlenmiştir. Bu sonuç hizmet süresi değişkeninin üniversitede görev yapan akademik ve idari personelin saldırı ve tehditler ile kişisel verilerin korunmasına yönelik farkındalığı üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Örgütsel iletişimin informel iletişim boyutu hizmet süresine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın 5-10 yıl ve 11-20 yıl ile 5-10 yıl ve 21-30 yıl olan katılımcılar arasında olduğu belirlenmiştir. Bu fark hizmet süresi 5 -10 yıl olan katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .037 olduğu belirlenmiştir. Bu sonuç hizmet süresi değişkeninin üniversitede görev yapan akademik ve idari personelin informel iletişimi üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Bilgi paylaşımı hizmet süresine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın 5 yıldan az ve 11-20 yıl, 5 yıldan az ve 21-30 yıl ile 5 yıldan az ve 30 yıl ve üzeri olan gruplar arasında olduğu belirlenmiştir. Bu fark hizmet süresi 5 yıldan az olan katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .040 olduğu bulgulanmıştır. Bu sonuca göre hizmet süresi değişkeninin üniversitede görev yapan akademik ve idari personelin bilgi paylaşımı üzerinde orta büyüklükte etkiye sahip olduğu belirlenmiştir

Bilgi paylaşımının alt boyutları örtük bilgi paylaşımı ve açık bilgi paylaşımı hizmet süresine anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın 5 yıldan az ve 11-20 yıl, 5 yıldan az ve 21-30 yıl ile 5 yıldan az ve 30 yıl ve üzeri olan gruplar arasında olduğu belirlenmiştir. Bu fark hizmet süresi 5 yıldan az olan katılımcıların lehinedir. Hizmet süresi değişkenin açık ve örtük bilgi paylaşımına etkisi açısından elde edilen eta kare (η2) değerinin .022 ve .045 olduğu bulgulanmıştır. Bu sonuca göre hizmet süresi değişkeninin üniversitede görev yapan akademik ve idari personelin açık ve örtük bilgi paylaşımları üzerinde orta büyüklükte etkiye sahip olduğu belirlenmiştir.

4.2.4. Araştırma Değişkenlerinin İnternette/ Sosyal Ağ Sitelerinde Gizlilik/Güvenlik Ayarlarını Kontrol Etme Sıklığına Göre Farklılık Analizi Sonuçları

Bu başlık altında katılımcıların kurumsal bilgi güvenliği, bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı değişkenlerinin İnternette/ sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre farklılık analizi sonuçları yer almaktadır.

Tablo 13. Katılımcıların Görüşlerinin İnternette/ Sosyal Ağ Sitelerinde Gizlilik/Güvenlik Ayarlarını Kontrol Etme Sıklığı Değişkenine Göre Karşılaştırılması

Değişken	Gizlilik/ Güvenlik Kontrol Sıklığı	N	$\bar{X}$	SS	F	p	Fark	η2
Kurumsal Bilgi Güvenliği	A. Ayda birkaç defa	79	3.61	.683	4.718	.001	A>E B>E	.038
	B. Ayda bir	67	3.57	.507				
	C. Yılda birkaç defa	115	3.47	.515				
	D. Yılda bir	67	3.40	.486				
	E. Kontrol etmiyorum	151	3.33	.483				
Kurumsal Bilgi Güvenliği Ölçeği Alt Boyutları								
Bilgi Güvenliği Kültürü Boyutu	A. Ayda birkaç defa	79	3.63	.846	4.785	.001	A>E B>E	.038
	B. Ayda bir	67	3.54	.692				
	C. Yılda birkaç defa	115	3.43	.701				
	D. Yılda bir	67	3.35	.651				
	E. Kontrol etmiyorum	151	3.25	.625				
Bilgi Güvenliği Uygulaması Boyutu	A. Ayda birkaç defa	79	3.51	.757	3.862	.004	A>E	.031
	B. Ayda bir	67	3.39	.622				
	C. Yılda birkaç defa	115	3.35	.556				
	D. Yılda bir	67	3.29	.545				
	E. Kontrol etmiyorum	151	3.19	.551				

Bilgi Güvenliği Yaklaşımı Boyutu	A. Ayda birkaç defa	79	3.56	.805	3.124	.015	A>E	.025
	B. Ayda bir	67	3.54	.659				
	C. Yılda birkaç defa	115	3.39	.637				
	D. Yılda bir	67	3.45	.609				
	E. Kontrol etmiyorum	151	3.28	.600				
Bilgi Güvenliği Yönetimi Boyutu	A. Ayda birkaç defa	79	3.61	.727	5.414	.000	A>E A>D B>D B>E	.043
	B. Ayda bir	67	3.59	.583				
	C. Yılda birkaç defa	115	3.49	.579				
	D. Yılda bir	67	3.30	.551				
	E. Kontrol etmiyorum	151	3.31	.555				
Bilgi Güvenliğinde Gizlilik Boyutu	A. Ayda birkaç defa	79	3.87	.793	.450	.773		
	B. Ayda bir	67	3.94	.618				
	C. Yılda birkaç defa	115	3.81	.694				
	D. Yılda bir	67	3.91	.685				
	E. Kontrol etmiyorum	151	3.84	.696				
Bilgi Güvenliği Farkındalığı	A. Ayda birkaç defa	79	3.72	.679	7.650	.000	A>D A>E B>E C>E	.060
	B. Ayda bir	67	3.64	.528				
	C. Yılda birkaç defa	115	3.63	.577				
	D. Yılda bir	67	3.42	.498				
	E. Kontrol etmiyorum	151	3.37	.527				
Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği Alt Boyutları								
Saldırı ve Tehditler Boyutu	A. Ayda birkaç defa	79	3.49	.797	6.188	.000	A>E A>D C>E	.049
	B. Ayda bir	67	3.32	.625				
	C. Yılda birkaç defa	115	3.35	.647				
	D. Yılda bir	67	3.14	.559				
	E. Kontrol etmiyorum	151	3.10	.587				
Kişisel Verilerin Korunması Boyutu	A. Ayda birkaç defa	79	3.93	.654	6.993	.000	A>E B>E C>E	.055
	B. Ayda bir	67	3.93	.544				
	C. Yılda birkaç defa	115	3.88	.608				
	D. Yılda bir	67	3.67	.538				
	E. Kontrol etmiyorum	151	3.60	.586				
Örgütsel İletişim	A. Ayda birkaç defa	79	3.64	.682	2.172	.071		
	B. Ayda bir	67	3.50	.572				
	C. Yılda birkaç defa	115	3.48	.568				
	D. Yılda bir	67	3.46	.603				
	E. Kontrol etmiyorum	151	3.38	.651				

Örgütsel İletişim Ölçeği Alt Boyutları								
Formel İletişim Boyutu	A. Ayda birkaç defa	79	3.64	.682	2.172	.071		
	B. Ayda bir	67	3.50	.572				
	C. Yılda birkaç defa	115	3.48	.568				
	D. Yılda bir	67	3.46	.603				
	E. Kontrol etmiyorum	151	3.38	.651				
İnformel İletişim Boyutu	A. Ayda birkaç defa	79	3.05	.595	3.015	.018	A>E	.024
	B. Ayda bir	67	3.01	.564				
	C. Yılda birkaç defa	115	2.88	.590				
	D. Yılda bir	67	2.86	.533				
	E. Kontrol etmiyorum	151	2.81	.540				
Bilgi Paylaşımı	A. Ayda birkaç defa	79	3.54	.619	3.557	.007	A>E B>E	.029
	B. Ayda bir	67	3.55	.542				
	C. Yılda birkaç defa	115	3.43	.548				
	D. Yılda bir	67	3.33	.488				
	E. Kontrol etmiyorum	151	3.32	.542				
Bilgi Paylaşım Ölçeği Alt Boyutları								
Açık Bilgi Paylaşımı Boyutu	A. Ayda birkaç defa	79	3.42	.759	1.818	.124		
	B. Ayda bir	67	3.46	.719				
	C. Yılda birkaç defa	115	3.31	.667				
	D. Yılda bir	67	3.31	.572				
	E. Kontrol etmiyorum	151	3.23	.641				
Örtük Bilgi Paylaşımı Boyutu	A. Ayda birkaç defa	79	3.61	.659	3.907	.004	A>E	.031
	B. Ayda bir	67	3.60	.574				
	C. Yılda birkaç defa	115	3.50	.585				
	D. Yılda bir	67	3.34	.538				
	E. Kontrol etmiyorum	151	3.37	.561				

Tablo 13 incelendiği araştırma değişkenlerinin İnternette/ sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığına göre anlamlı farklılık gösterdiği belirlenmiştir. Grupların homojen dağılması nedeniyle farklılığın hangi sıklıkla kontrol eden gruplar arasında olduğunu belirlemek amacıyla post-hoc analizlerinden Scheffe testi yapılmıştır. Ayrıca İnternette/ sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkeninin etki düzeyini belirlemek için eta kare (η2) değeri hesaplanmıştır.

Araştırma değişkenleri arasında yer alan kurumsal bilgi güvenliği İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın "ayda birkaç defa" ve "kontrol etmiyorum" ile "ayda bir defa" ve "kontrol etmiyorum" yanıtını veren gruplar arasında olduğu belirlenmiş ve bu fark İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını "ayda birkaç defa" ve "ayda bir defa" kontrol eden katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .038 olduğu belirlenmiştir. Bu sonuç İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkeninin üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Kurumsal bilgi güvenliği ölçeğinin bilgi güvenliğinde gizlilik alt boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermemektedir ancak kurumsal bilgi güvenliği ölçeğinin bilgi güvenliği kültürü boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın "ayda birkaç defa" ve "kontrol etmiyorum" ile "ayda bir defa" ve "kontrol etmiyorum" yanıtını veren gruplar arasında olduğu belirlenmiş ve bu fark İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını "ayda birkaç defa" ve "ayda bir defa" kontrol eden katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .038 olduğu belirlenmiştir. Bu sonuç İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkeninin üniversitede görev yapan akademik ve idari personelin bilgi güvenliği kültürü üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Kurumsal bilgi güvenliği ölçeğinin bilgi güvenliği uygulaması boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın "ayda birkaç defa" ve "kontrol etmiyorum" yanıtını veren gruplar arasında olduğu belirlenmiş ve bu fark İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını "ayda birkaç defa" kontrol eden katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .031 olduğu belirlenmiştir. Bu sonuç İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkeninin üniversitede görev yapan akademik ve idari personelin bilgi güvenliği uygulaması üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Kurumsal bilgi güvenliği ölçeğinin bilgi güvenliği yaklaşımı boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın "ayda birkaç defa" ve "kontrol etmiyorum" yanıtını veren gruplar arasında olduğu belirlenmiş ve bu fark İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını "ayda birkaç defa" kontrol eden katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .025 olduğu bulgulanmıştır. Bu sonuca göre İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkeninin üniversitede görev yapan akademik ve idari personelin bilgi güvenliği yaklaşımı üzerinde orta büyüklükte etkiye sahip olduğu belirlenmiştir.

Kurumsal bilgi güvenliği ölçeğinin bilgi güvenliği yönetimi boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın "ayda birkaç defa" ve "kontrol etmiyorum", "ayda birkaç defa" ve "yılda bir defa", "ayda bir" ve "kontrol etmiyorum" ile "ayda bir" ve "yılda bir defa" yanıtını veren gruplar arasında olduğu belirlenmiştir. Bu fark İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını "ayda birkaç defa" ve "ayda bir defa" kontrol eden katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .043 olduğu belirlenmiştir. Bu sonuç İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkeninin üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği ölçeğinin bilgi güvenliği yönetimi üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Bilgi güvenliği farkındalığı İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın "ayda birkaç defa" ve "kontrol etmiyorum", "ayda birkaç defa" ve "yılda bir defa", "ayda bir" ve

“kontrol etmiyorum” ile “yılda birkaç defa” ve “kontrol etmiyorum” yanıtını veren gruplar arasında olduğu belirlenmiştir. Bu fark İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını “ayda birkaç defa”, “ayda bir” ve “yılda birkaç defa” kontrol eden katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .060 olduğu belirlenmiştir. Bu sonuç göre İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkeninin üniversitede görev yapan akademik ve idari personelin bilgi güvenliği farkındalığı üzerinde orta büyüklükte etkiye sahip olduğu belirlenmiştir.

Bilgi güvenliği farkındalığı ölçeğinin saldırı ve tehditler boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın “ayda birkaç defa” ve “kontrol etmiyorum”, “ayda birkaç defa” ve “yılda bir defa”, “ayda bir defa” ve “kontrol etmiyorum” ile yılda birkaç defa ve “kontrol etmiyorum” yanıtını veren gruplar arasında olduğu belirlenmiştir. Bu fark İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını “ayda birkaç defa” ve “ayda bir defa” kontrol eden katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .049 olduğu belirlenmiştir. Bu sonuç İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkeninin üniversitede görev yapan akademik ve idari personelin saldırı ve tehditler farkındalığı üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Bilgi güvenliği farkındalığı ölçeğinin kişisel verilerin korunması boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın “ayda birkaç defa” ve “kontrol etmiyorum”, ayda bir ve “kontrol etmiyorum” ile “yılda birkaç defa” ve “kontrol etmiyorum” yanıtını veren gruplar arasında olduğu belirlenmiş ve bu fark İnternette/ sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını “ayda birkaç defa”, ayda bir ve yılda birkaç defa kontrol eden katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .055 olduğu belirlenmiştir. Bu sonuca göre İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkeninin üniversitede görev yapan akademik ve idari personelin kişisel verilerin korunmasına yönelik farkındalığı üzerinde orta büyüklükte etkiye sahip olduğu belirlenmiştir.

Örgütsel iletişim ölçeği ve formel iletişim alt boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermemektedir ancak ölçeğin informel iletişim boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın “ayda birkaç defa” ve “kontrol etmiyorum” yanıtını veren gruplar arasında olduğu belirlenmiş ve bu fark İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını “ayda birkaç defa” kontrol eden katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2) değerinin .024 olduğu belirlenmiştir. Bu sonuç göre İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkeninin üniversitede görev yapan akademik ve idari personelin informel iletişimi üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

Üniversitede görev yapan akademik ve idari personelin bilgi paylaşımı İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın “ayda birkaç defa” ve “kontrol etmiyorum” ile ayda bir defa ve “kontrol etmiyorum” yanıtını veren gruplar arasında olduğu belirlenmiş ve bu fark İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını “ayda birkaç defa” ve ayda bir defa kontrol eden katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare (η2)

değerinin .029 olduğu belirlenmiştir. Bu sonuç göre İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkeninin üniversitede görev yapan akademik ve idari personelin bilgi paylaşımı üzerinde orta büyüklükte etkiye sahip olduğu belirlenmiştir.

Bilgi paylaşım ölçeğinin açık bilgi paylaşımı İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermemektedir ancak örtük bilgi paylaşımı İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermektedir. Analiz sonucunda farklılığın "ayda birkaç defa" ve "kontrol etmiyorum" yanıtını veren gruplar arasında olduğu belirlenmiş ve bu fark İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını "ayda birkaç defa" kontrol eden katılımcıların lehinedir. Etki değerini belirlemek için hesaplanan eta kare ($\eta 2$) değerinin .031 olduğu belirlenmiştir. Bu sonuç İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkeninin üniversitede görev yapan akademik ve idari personelin örtük bilgi paylaşımı üzerinde orta büyüklükte etkiye sahip olduğunu göstermektedir.

4.3. Kurumsal Bilgi Güvenliği, Bilgi Güvenliği Farkındalığı, Örgütsel İletişim ve Örgütsel Bilgi Paylaşımı Değişkenleri Arasındaki İlişkiler

Bu bölümde araştırmaya katılan akademik ve idari personelin kurumsal bilgi güvenliği, bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı değişkenleri arasındaki ilişkiyi belirlemek için yapılan korelasyon analizine yönelik bulgular ve yorumlara yer verilmiştir. Korelasyon analizi sonucunda elde edilen bulgular Tablo 14'te sunulmuştur.

Tablo 14. Araştırma Değişkenleri Arasındaki Korelasyon Analizi

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1.Kurumsal Bilgi Güvenliği	1														
2.Bilgi Güvenliği Farkındalığı	.725**	1													
3. Örgütsel İletişim	.646**	.559**	1												
4.Bilgi Paylaşımı	.658**	.588**	.732**	1											
5.Bilgi Güvenliği Kültürü Boyutu	.861**	.640**	.596**	.583**	1										
6.Bilgi Güvenliği Uygulaması Boyutu	.885**	.661**	.547**	.581**	.730**	1									
7.Bilgi Güvenliği Yaklaşımı Boyutu	.866**	.615**	.536**	.564**	.684**	.730**	1								
8.Bilgi Güvenliği Yönetimi Boyutu	.913**	.661**	.616**	.610**	.723**	.731**	.754**	1							
9.Bilgi Güvenliğinde Gizlilik Boyutu	.506**	.323**	.272**	.294**	.280**	.348**	.375**	.363**	1						
10.Saldırı ve Tehditler Boyutu	.648**	.917**	.493**	.544**	.579**	.611**	.553**	.591**	.236**	1					
11.Kişisel Verilerin Korunması Boyutu	.685**	.923**	.535**	.538**	.598**	.605**	.577**	.624**	.355**	.692**	1				
12.Formel İletişim Boyutu	.646**	.559**	1.000**	.732**	.596**	.547**	.536**	.616**	.272**	.493**	.535**	1			
13.İnformel İletişim Boyutu	.422**	.402**	.357**	.517**	.345**	.373**	.413**	.398**	.153**	.402**	.339**	.357**	1		
14.Açık Bilgi Paylaşımı Boyutu	.538**	.496**	.626**	.838**	.508**	.491**	.486**	.467**	.204**	.483**	.430**	.626**	.457**	1	
15.Örtük Bilgi Paylaşımı Boyutu	.623**	.548**	.676**	.934**	.533**	.539**	.519**	.599**	.302**	.491**	.516**	.676**	.468**	.589**	1

**p<0.01; N= 479

Tablo 14 incelendiğinde, üniversitede görev yapan personelin kurumsal bilgi güvenliği ile saldırı ve tehditler (r= 0.648; p=0.000<0.05), kişisel verilerin korunması (r= 0.685; p=0.000<0.05), formel iletişim (r= 0.646; p=0.000<0.05), informel iletişim (r= 0.422; p=0.000<0.05), açık bilgi paylaşımı (r= 0.538; p=0.000<0.05) ve örtük bilgi paylaşımı (r= 0.623; p=0.000<0.05) arasında pozitif yönde orta düzey anlamlı bir ilişki olduğu görülmektedir. Bu sonuca göre kurumsal bilgi güvenliği arttıkça araştırma değişkenlerinin düzeyi de artmaktadır.

Araştırmaya katılan akademik ve idari personelin, kişisel verilerin korunması, saldırı ve tehditler, formel iletişim, informel iletişim, açık bilgi paylaşımı, örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerindeki yordayıcılık gücünü belirlemek amacı ile çoklu regresyon analizi gerçekleştirilmiştir. Analiz sonucunda elde edilen değerler Tablo 15'te sunulmuştur.

Tablo 15. Kurumsal Bilgi Güvenliğinin Yordanmasına İlişkin Regresyon Analizi Sonuçları

Yordayıcı Değişkenler	**R**	**R^2**	**R^2 Değişikliği (ΔR^2)**	**B**	**Standart Hata**	**β**	**t**	**p**
Standart	.796	.634	.629	.412	.113		3.662	.000
Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği Alt Boyutları								
Kişisel Verilerin Korunması Boyutu				.167	.034	.203	4.956	.000
Saldırı ve Tehditler Boyutu				.268	.037	.300	7.321	.000
Örgütsel İletişim Ölçeği Alt Boyutları								
Formel İletişim				.196	.037	.225	5.327	.000
İnformel İletişim				.058	.031	.061	1.839	.067
Bilgi Paylaşım Ölçeği Alt Boyutları								
Açık Bilgi Paylaşımı				.039	.031	.049	1.251	.212
Örtük Bilgi Paylaşımı				.146	.038	.159	3.828	.000

Analiz sonuçları incelendiğinde, kişisel verilerin korunması, saldırı ve tehditler, formel iletişim, informel iletişim, açık bilgi paylaşımı, örtük bilgi paylaşımının kurumsal bilgi güvenliğinin anlamlı yordayıcısı olduğu belirlenmiştir (R=.79 R2=.63, ΔR2=.62, p<.01). Araştırma kapsamında kullanılan değişkenlerin regresyon katsayıları incelendiğinde, kişisel verilerin korunması (β= .203, p<.01), saldırı ve tehditler (β= .300, p<.01), formel iletişim (β= .225, p<.01) ve örtük bilgi paylaşımı (β= .159, p<.01) değişkenlerinin kurumsal bilgi güvenliğinin anlamlı bir yordayıcısı olduğu görülmüştür. Ancak informel iletişim (β= .06, p>.01) ve açık bilgi paylaşımı (β= .04, p>.01) değişkenleri kurumsal bilgi güvenliği üzerinden anlamlı bir etkisi olmadığı belirlenmiştir. Araştırma kapsamında incelenen tüm değişkenler kurumsal bilgi güvenliğine ilişkin varyansın %63'ünü açıklamaktadır.

4.4. Araştırma Modelinin YEM Analizi Sonuçları Çerçevesinde Ortaya Çıkan Uyum İyiliği Değerleri ve Karşılaştırma Ölçütleri

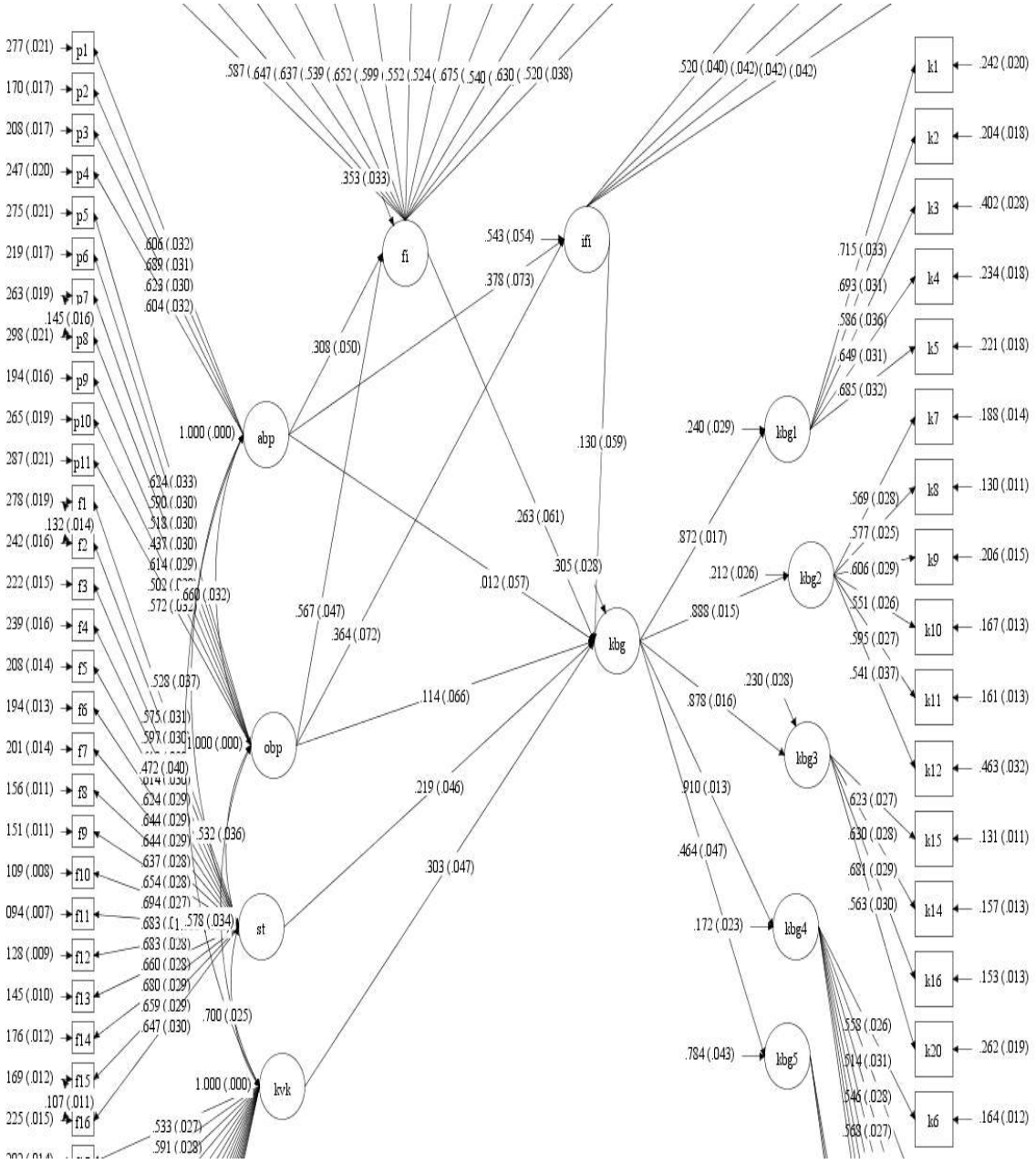
Yapısal eşitlik modellemesi analizi kullanılarak kişisel verilerin korunması, saldırı ve tehditler, formel iletişim, informel iletişim, açık bilgi paylaşımı, örtük bilgi paylaşımı ve kurumsal bilgi güvenliği arasındaki açıklayıcı ve yordayıcı ilişkiler incelenmiştir. Analiz sonucunda elde edilen modelin uyum değerleri Tablo 16'da sunulmuştur.

Tablo 16. Araştırma Modeline Ait Uyum Değerleri

Modele Ait Uyum Değerleri	χ2	sd	χ2 /sd	RMSEA	SRMR	CFI	TLI
	7119.487	3628	1.962	0.045	0.050	0.896	0.893

İlgili alan yazın ve literatürde yapılan araştırmalar temel alınarak geliştirilen modele ilişkin değerler incelendiğinde, test edilen modelin mükemmel ve kabul edilebilir uyum değerlerine sahip olduğu belirlenmiştir (Hu ve Bentler, 1999: 13-15; Sümer, 2000: 72; Kline, 2015, 270-280).

"Kişisel verilerin korunması, saldırı ve tehditler, formel iletişim, informel iletişim, açık bilgi paylaşımı, örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerinde pozitif etkisi vardır" hipotezinin sınanması ve diğer değişkenler üzerindeki doğrudan ve dolaylı etkilerinin belirlenmesi amacıyla yol analizi yapılmıştır. Yol analizi sonucunda belirlenen model Şekil 6'da görülmektedir.



Şekil 6. Araştırma Modeline İlişkin Yol Analizi Modeli

Şekil 6'da yer alan kısaltmalara ilişkin açıklamalar maddeler halinde sunulmuştur:

KBG: Kurumsal Bilgi Güvenliği

KBG1: Kurumsal Bilgi Güvenliği Ölçeğinin Bilgi Güvenliği Kültürü Boyutu

KBG2: Kurumsal Bilgi Güvenliği Ölçeğinin Bilgi Güvenliği Uygulaması Boyutu

KBG3: Kurumsal Bilgi Güvenliği Ölçeğinin Bilgi Güvenliği Yaklaşımı Boyutu

KBG4: Kurumsal Bilgi Güvenliği Ölçeğinin Bilgi Güvenliği Yönetimi Boyutu

KBG5: Kurumsal Bilgi Güvenliği Ölçeğinin Bilgi Güvenliğinde Gizlilik Boyutu

ST: Kişisel Bilgi Güvenliği Farkındalığı Ölçeğinin Saldırı ve Tehditler Boyutu

KVK: Kişisel Bilgi Güvenliği Farkındalığı Ölçeğinin Kişisel Verilerin Korunması Boyutu

Fİ: Örgütsel İletişim Ölçeğinin Formel İletişim Boyutu

İFİ: Örgütsel İletişim Ölçeğinin İnformel İletişim Boyutu

ABP: Bilgi Paylaşımı Ölçeğinin Açık Bilgi Paylaşımı Boyutu

ÖBP: Bilgi Paylaşımı Ölçeğinin Örtük Bilgi Paylaşımı Boyutu

Modelde test edilen değişkenlerin doğrudan ve dolaylı etkilerin ortaya çıkarılması amacıyla bootstrap analizi gerçekleştirilmiştir. Analiz sonuçları ve güven aralıkları Tablo 17'de sunulmuştur.

Tablo 17. Modelde Yer Alan Değişkenler Arasındaki Etkiler

				95% Güven Aralığı			
	Tahmini Değer	**Standart Hata**	**t**	**Düşük**	**Yüksek**	**R^2**	**p**
Toplam etki							
Açık Bilgi Paylaşımı → Kurumsal Bilgi Güvenliği	0.141	0.052	2.700	0.048	0.226	0.695	0.007
Örtük Bilgi Paylaşımı→ Kurumsal Bilgi Güvenliği	0.310	0.057	5.452	0.205	0.382		0.000
Dolaylı etki							
Açık Bilgi Paylaşımı → Kurumsal Bilgi Güvenliği	0.130	.0410	3.180	0.035	0.178		0.001
Örtük Bilgi Paylaşımı→ Kurumsal Bilgi Güvenliği	0.196	0.055	3.559	0.070	0.279		0.000
Toplam doğrudan etki							
Saldırı ve Tehditler → Kurumsal Bilgi Güvenliği	0.219	0.053	4.133	0.134	0.305		0.000
Kişisel Verilerin Korunması → Kurumsal Bilgi Güvenliği	0.303	0.056	5.431	0.206	0.391		0.000
Açık Bilgi Paylaşımı → Kurumsal Bilgi Güvenliği	0.012	0.061	0.188	-0.089	0.119		0.854
Örtük Bilgi Paylaşımı→ Kurumsal Bilgi Güvenliği	0.114	0.081	1.404	-0.013	0.255		0.161
Formel İletişim → Kurumsal Bilgi Güvenliği	0.263	0.070	3.752	0.133	0.376		0.000
İnformel İletişim → Kurumsal Bilgi Güvenliği	0.130	0.065	1.987	0.021	0.230		0.061
Açık Bilgi Paylaşımı → Formel İletişim	0.308	0.057	5.352	0.210	0.403	0.647	0.000
Örtük Bilgi Paylaşımı → Formel İletişim	0.567	0.052	10.838	0.481	0.652		0.000
Açık Bilgi Paylaşımı → İnformel İletişim	0.378	0.078	4.848	0.227	0.505	0.457	0.000
Örtük Bilgi Paylaşımı → İnformel İletişim	0.364	0.076	4.791	0.249	0.488		0.000
Özel Dolaylı Etki							
Açık Bilgi Paylaşımı → Formel İletişim → Kurumsal Bilgi Güvenliği	0.081	0.027	3.005	0.038	0.127		0.003
Açık Bilgi Paylaşımı → İnformel İletişim → Kurumsal Bilgi Güvenliği	0.049	0.028	1.772	0.007	0.096		0.076
Örtük Bilgi Paylaşımı → Formel İletişim → Kurumsal Bilgi Güvenliği	0.149	0.042	3.560	0.076	0.217		0.000
Örtük Bilgi Paylaşımı → İnformel İletişim → Kurumsal Bilgi Güvenliği	0.047	0.026	1.845	0.007	0.089		0.065

Analiz sonucunda kişisel bilgi güvenliği farkındalığı ölçeğinin saldırı ve tehditler boyutunun üniversitelerde görev yapan akademik ve idari personelin kurumsal bilgi güvenliği üzerinde anlamlı ve pozitif bir etkiye sahip olduğu belirlenmiştir (β = .219, p <.01). "Saldırı ve tehditlere yönelik farkındalığının kurumsal bilgi güvenliği üzerinde pozitif etkisi bulunmaktadır." hipotezini doğrulamaktadır.

Analiz sonucunda kişisel bilgi güvenliğine yönelik farkındalığının kişisel verilerin korunmasına yönelik farkındalığının üniversitelerde görev yapan akademik ve idari personelin kurumsal bilgi güvenliği üzerinde anlamlı ve pozitif bir etkiye sahip olduğu belirlenmiştir (β = .303, p <.01). "Kişisel verilerin korunmasına yönelik farkındalığının kurumsal bilgi güvenliği üzerinde pozitif etkisi bulunmaktadır." hipotezini doğrulamaktadır.

Formel iletişimin üniversitelerde görev yapan akademik ve idari personelin kurumsal bilgi güvenliği üzerinde anlamlı ve pozitif bir etkiye sahip olduğu belirlenmiştir (β = .263, p <.01). "Formel iletişimin kurumsal bilgi güvenliği üzerinde pozitif etkisi bulunmaktadır." hipotezini doğrulamaktadır.

Analiz sonucunda informel iletişimin üniversitelerde görev yapan akademik ve idari personelin kurumsal bilgi güvenliğini anlamlı olarak etkilememektedir (β = .130, p >.05). "İnformel iletişimin kurumsal bilgi güvenliği üzerinde pozitif etkisi bulunmaktadır." hipotezi reddedilmiştir.

Açık bilgi paylaşımının üniversitelerde görev yapan akademik ve idari personelin kurumsal bilgi güvenliğini anlamlı olarak etkilemediği belirlenmiştir (β = .012, p >.05). "Açık bilgi paylaşımının kurumsal bilgi güvenliği üzerinde pozitif etkisi bulunmaktadır." hipotezi reddedilmiştir.

Örtük bilgi paylaşımının üniversitelerde görev yapan akademik ve idari personelin kurumsal bilgi güvenliğini anlamlı olarak etkilemediği belirlenmiştir (β = .114, p >.05). "Örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerinde pozitif etkisi bulunmaktadır." hipotezi reddedilmiştir.

Açık bilgi paylaşımının üniversitelerde görev yapan akademik ve idari personelin formel iletişimi üzerinde anlamlı ve pozitif etkisi bulunmaktadır (β = .308, p <.01). "Açık bilgi paylaşımının formel iletişim üzerinde pozitif etkisi bulunmaktadır." hipotezini doğrulamaktadır.

Açık bilgi paylaşımının üniversitelerde görev yapan akademik ve idari personelin informel iletişimi üzerinde anlamlı ve pozitif etkisi bulunmaktadır (β = .378, p <.01). "Açık bilgi paylaşımının informel iletişim üzerinde pozitif etkisi bulunmaktadır." hipotezini doğrulamaktadır.

Örtük bilgi paylaşımının üniversitelerde görev yapan akademik ve idari personelin formel iletişimi üzerinde anlamlı ve pozitif etkisi bulunmaktadır (β = .567, p <.01). "Örtük bilgi paylaşımının formel iletişim üzerinde pozitif etkisi bulunmaktadır." hipotezini doğrulamaktadır.

Örtük bilgi paylaşımının üniversitelerde görev yapan akademik ve idari personelin informel iletişimi üzerinde anlamlı ve pozitif etkisi bulunmaktadır (β = .364, p <.01). "Örtük bilgi paylaşımının informel iletişim üzerinde pozitif etkisi bulunmaktadır." hipotezini doğrulamaktadır.

Açık bilgi paylaşımının kurumsal bilgi güvenliği üzerinde doğrudan etkisi olmamasına rağmen dolaylı etkisi olduğu belirlenmiştir (β = .130, p <.01). "Açık bilgi paylaşımı kurumsal bilgi güvenliği üzerinde dolaylı etkisi bulunmaktadır." hipotezini doğrulamaktadır.

Örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerinde doğrudan etkisi olmamasına rağmen dolaylı etkisi olduğu belirlenmiştir (β = .196, p <.01). "Örtük bilgi paylaşımı kurumsal bilgi güvenliği üzerinde dolaylı etkisi bulunmaktadır." hipotezini doğrulamaktadır

Analiz sonucunda formel iletişimin açık bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi olduğu belirlenmiştir (β = .081, p <.01). "Formel iletişimin açık bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi bulunmaktadır" hipotezi kabul edilmiştir.

Analiz sonucunda informel iletişimin açık bilgi paylaşımının kurumsal bilgi güvenliğini anlamlı olarak etkilemediği belirlenmiştir (β = .049, p >.05). "İnformel iletişimin açık bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi bulunmaktadır" hipotezi reddedilmiştir.

Analiz sonucunda formel iletişimin örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi olduğu belirlenmiştir (β = .149, p <.01). "Formel iletişimin örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi bulunmaktadır" hipotezi kabul edilmiştir.

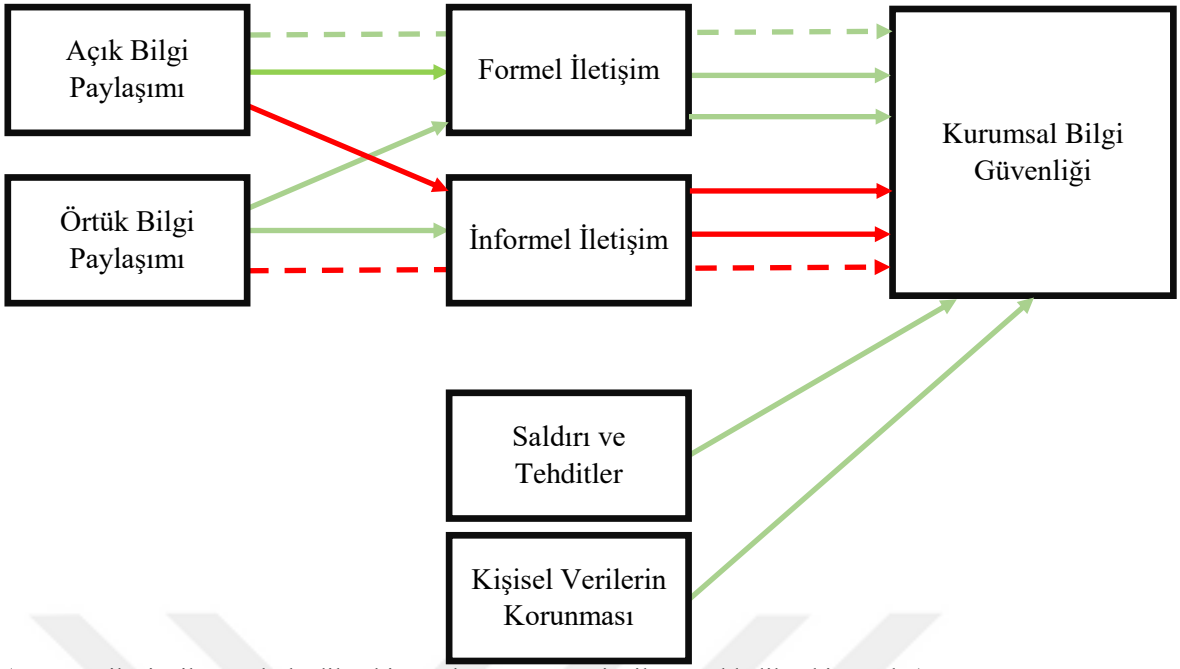
Analiz sonucunda informel iletişimin örtük bilgi paylaşımının kurumsal bilgi güvenliğini anlamlı olarak etkilemediği belirlenmiştir (β = .049, p >.05). "İnformel iletişimin örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi bulunmaktadır" hipotezi reddedilmiştir.

Formel iletişim açık ve örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi bulunmaktadır. Ancak informel iletişimin açık ve örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi bulunmamaktadır.

Araştırma kapsamında test edilen hipotezlere ilişkin sonuçlar Tablo 18'de sunulmuştur.

Tablo 18. Araştırma Hipotezlerinin Analiz Sonucu

H1: Saldırı ve tehditlere yönelik farkındalığı kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler.	Kabul edilmiştir.
H2: Kişisel verilerin korunmasına yönelik farkındalığı kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler.	Kabul edilmiştir.
H3: Formel iletişim kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler.	Kabul edilmiştir.
H4: İnformel iletişim kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler.	Reddedilmiştir.
H5: Açık bilgi paylaşımı kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler.	Reddedilmiştir.
H6: Örtük bilgi paylaşımı kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler.	Reddedilmiştir.
H7: Açık bilgi paylaşımı formel iletişim düzeyini pozitif ve anlamlı etkiler.	Kabul edilmiştir.
H8: Açık bilgi paylaşımı informel iletişim düzeyini pozitif ve anlamlı etkiler.	Kabul edilmiştir.
H9: Örtük bilgi paylaşımı formel iletişim düzeyini pozitif ve anlamlı etkiler.	Kabul edilmiştir.
H10: Örtük bilgi paylaşımı informel iletişim düzeyini pozitif ve anlamlı etkiler.	Kabul edilmiştir.
H11: Açık bilgi paylaşımı kurumsal bilgi güvenliğini dolaylı etkiler.	Kabul edilmiştir.
H12: Örtük bilgi paylaşımı kurumsal bilgi güvenliğini dolaylı etkiler.	Kabul edilmiştir.
H13: Formel iletişimin açık bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi vardır.	Kabul edilmiştir.
H14: İnformel iletişimin açık bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi vardır.	Reddedilmiştir.
H15: Formel iletişimin örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi vardır.	Kabul edilmiştir.
H16:İnformel iletişimin örtük bilgi paylaşımının kurumsal bilgi güvenliği üzerinde aracılık etkisi vardır.	Reddedilmiştir.



(Not: Yeşil Çizgiler: Kabul edilen hipotezler; Kırmızı Çizgiler: Reddedilen hipotezler)

Şekil 7. Araştırma Modeline İlişkin Yol Analizi Sonucu

4.5. Kurumsal Bilgi Güvenliğinin Veri Madenciliği Yöntemi İle Tahmin Başarımına İlişkin Bulgular

Kişisel verilerin korunması, saldırı ve tehditler, formel iletişim, informel iletişim, açık bilgi paylaşımı, örtük bilgi paylaşımının kurumsal bilgi güvenliğinin veri madenciliği ile tahmin başarımını belirlemek amacıyla yapılan analiz sonuçları Tablo 19'da sunulmuştur. Kişisel verilerin korunması, saldırı ve tehditler, formel iletişim, informel iletişim, açık bilgi paylaşımı, örtük bilgi paylaşımı giriş değişkeni olarak, kurumsal bilgi güvenliği çıkış değişkeni olarak belirlenmiştir.

Tablo 19. Kurumsal Bilgi Güvenliği Tahmin Başarımına Yönelik Performans Vektör Değerleri

	Yapay Sinir Ağları	**Destek Vektör Makineleri**	**K-En Yakın Komşu**	**Rastgele Orman**
Ortalama Karekök Hata	.330 ± .045	.332± .039	.336 ± .034	.330 ± .048
Mutlak Hata	.258± .038	.261± .034	.261± .027	.257± .037
Korelasyon	.790 ± .060	.783 ± .059	.780 ± .075	.783 ± .073

Tablo 19 incelendiğinde Yapay Sinir Ağları tahmin değerinin .790, Destek Vektör Makineleri tahmin değerinin .783, K-En Yakın Komşu tahmin değerinin .780 ve Rastgele Orman tahmin değerinin .783 olduğu belirlenmiştir.

5. SONUÇ, TARTIŞMA VE ÖNERİLER

Kurumların işleyişini sürdürmesi, bilgi varlıklarını koruması için bilgi güvenliğinin sağlanması gerekli görülmektedir. Bilgi güvenliğinin sağlanması amacı ile teknolojik önlemler alınmaktadır. Ancak ilgili alan yazın incelendiğinde kurumsal bilgi güvenliğinin sağlanmasında yalnızca teknolojik önlemlerin yeterli olmadığına yönelik çalışmalara rastlanmıştır. Bilgi güvenliğinin sağlanmasında insan ve örgüt faktörü rol oynamaktadır. Bu bağlamda gerçekleştirilen araştırmada, üniversitelerde görev yapan akademik ve idari personelin kurumsal bilgi güvenliği, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı bağlamında incelenmiştir. Araştırma kapsamında, Bilgi Güvenliği Ölçeği (Gerçeker, 2012), Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği (Keser ve Güldüren, 2015) ile Türkçe uyarlaması Aslan (2014) tarafından yapılan Bilgi Paylaşım Ölçeği ayrıca Tuna (2008) tarafından geliştirilen standardizasyon işlemi araştırmacı tarafından gerçekleştirilen Örgütsel İletişim Envanteri kullanılmıştır. Ayrıca katılımcıların demografik bilgilerine yönelik bilgilere ulaşmak için ise Kişisel Bilgi Formu'ndan yararlanılmıştır. Araştırma kapsamında üniversitede görev yapan 527 akademik ve idari personelden veri toplanmıştır ancak eksik veya hatalı veri girişi nedeni ile analizler 479 veri üzerinden gerçekleştirilmiştir.

Araştırma sorularına yanıt aramak için çeşitli istatiksel analizler gerçekleştirilmiştir. Öncelikle verilerin normal dağılımını belirlemek amacı ile normallik testi gerçekleştirilmiştir. Analiz sonucunda, tüm ölçeklerin belirlenen normallik aralığında olduğu ve verilerin normal dağılım gösterdiği belirlenmiştir. Araştırma kapsamında korelasyon analizi, regresyon analizi, yapısal eşitlik modellemesi analizleri gerçekleştirilmiştir. Ayrıca veri madenciliğinin tahmin edici modellerinden, Destek Vektör Makineleri, Yapay Sinir Ağları, K- En Yakın Komşu ve Rastgele Orman algoritmaları kullanılmıştır.

Bu bölümde, araştırma sonucunda elde edilen bulgulara yönelik olarak ortaya çıkan sonuçlar ve tartışma sunulmuştur. Ayrıca araştırma sonuçları ışığında geliştirilen öneriler yer almaktadır.

5.1. Birinci Araştırma Problemine İlişkin Sonuç ve Tartışma

Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımına ilişkin algılarına yönelik analiz sonuçları ve yorumlar bu bölümde sunulmuştur.

Araştırma sonucunda üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği düzeyinin yüksek olduğu belirlenmiştir. İlgili alan yazın incelendiğinde benzer sonuçların yer aldığı görülmektedir. Gerçeker (2012), hastane çalışanları ile gerçekleştirdiği çalışmada bilgi güvenliği yönetimi, yaklaşımı, kültürü, gizliği, uygulaması boyutlarının yüksek düzeyde olduğu sonucuna ulaşmıştır. Turaç (2022) hemşirelerle gerçekleştirdiği çalışmada katılımcıların bilgi güvenliğinin orta düzeyin üzerinde olduğunu belirtmiştir. Ashenden (2018) gerçekleştirdiği çalışmada bu çalışma sonucunda elde edilen bulgulardan farklı sonuçlara ulaşmıştır. Gerçekleştirdiği araştırmada, kurumun bilgiyi koruma ihtiyacı nedeniyle yönlendirildiğini düşünen çalışanların, risklerin abartıldığını ve meslektaşlarının aşırı temkinli olduğunu düşündükleri sonucuna ulaşmıştır. Kurumların bilgi varlıklarının önemini giderek daha fazla farkına varması, dijital dönüşümle kurumsal bilgi güvenliğine yönelik gerçekleştirilen çalışmalar, kurumların kurumsal bilgi güvenliği standartlarına uymak amacıyla düzenledikleri

politikalar ve bu politikaların çalışanlarla paylaşılması gibi kurumsal bilgi güvenliğine yönelik gerçekleştirilen çalışmaların, olumlu sosyal etkilerin, motivasyon ve teşviklerin (Chan, Woon ve Kankanhalli, 2005; Gregory, 2003; Rezgui ve Marks, 2008; Kraemer vd., 2009; François, 2016; Parsons ve arkadaşları, 2015; Li vd., 2019) çalışanların kurumsal bilgi güvenliğinin yüksek olmasında olumlu etkisi olduğu düşünülebilir. Kurumların bilgi varlıklarının öneminin daha fazla farkına varması, bilgi güvenliği ihlali nedeniyle yaşanan olumsuzluklara ilişkin deneyimler veya duyumlar, çalışanların bilgi güvenliği bağlamında birbirlerinden olumlu etkilenmeleri, kurumsal işleyişte dijital dönüşümün yaşanması nedeniyle daha fazla bilişim teknolojileri cihazlarının kullanımının kurumsal bilgi güvenliğinin yüksek olmasıyla ilişkili olabilir. Bu sonuçlardan yola çıkarak üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliğinin yüksek olmasının üniversitelerin bilgi güvenliği ve bilgi varlıklarının korunması açısından olumlu bir durum olduğu söylenebilir.

Araştırma kapsamında incelenen üniversitede görev yapan akademik ve idari personelin bilgi güvenliği farkındalık düzeyinin yüksek olduğu belirlenmiştir. Alan yazın incelendiğinde araştırma sonucuna benzer sonuçların yer aldığı görülmektedir. Fakeh, Zulhemay, Shahibi ve Zaini (2012) kütüphanede çalışan personelle gerçekleştirdikleri çalışmada çalışanların bilgi güvenliği farkındalık düzeyinin yüksek olduğu sonucuna ulaşmışlardır. Öğretmenler üzerinde gerçekleştirilen bir çalışmada ise Canoğulları (2021) öğretmenlerin genel bilgi güvenliği farkındalığının orta düzeyin biraz üzerinde olduğunu belirtirken; Yılmaz, Şahin ve Akbulut (2016), öğretmenlerle gerçekleştirdikleri çalışmada, öğretmenlerin dijital veri güvenliği farkındalığının yüksek düzeyde olduğunu belirtmişlerdir. Karabatak ve Karabatak (2019) okul yöneticileri ile gerçekleştirdiği çalışmada, okul yöneticilerinin bilgi güvenliği farkındalığının orta düzeyin üzerinde olduğu sonucuna ulaşmışlardır. Ernita, Ruldeviyani, Maftuhah ve Mulyadi (2022) banka çalışanları ile gerçekleştirdikleri çalışmada çalışanların bilgi güvenliği farkındalık düzeyinin yüksek olduğunu belirtmişlerdir. Aslan (2017) Marmara Üniversitesinde çalışan akademik ve idari personelin bilgi güvenliği farkındalığının orta düzeyin üzerinde olduğu sonucuna ulaşmıştır. Benzer bir çalışmada Özdemir (2019) kamu kurumunda çalışan personelle gerçekleştirdiği çalışmada çalışanların kişisel verilerin korunması düzeyinin yüksek olduğunu belirtmiştir. Filik ve Ünalan (2021), kamu kurumunda çalışan personelle gerçekleştirdikleri çalışmada, kişisel verilerin korunması düzeyinin yüksek, saldırı ve tehditlere karşı farkındalık düzeyinin orta ve genel bilgi güvenliği farkındalık düzeyinin orta olduğu sonucuna ulaşmışlardır. Okul, Şimşek, Hafçı ve Barış (2018), konaklama işletmelerinde çalışan personelin bilgi güvenliği farkındalığının yüksek olduğunu belirtmişlerdir. Ancak ilgili alan yazında farklı sonuçlara da rastlanmıştır. Taner (2018) güvenlik güçleri ile gerçekleştirdiği çalışmada çalışanların bilgi güvenliği farkındalık düzeyinin ortalamanın altında olduğunu belirtmiştir. Alarifi, Tootell ve Hyland (2012) gerçekleştirdikleri çalışmada, katılımcıların bilgi güvenliği farkındalığının düşük olduğu sonucuna ulaşmışlardır. Araştırma bulgusu ve ilgili alan yazında yer alan çoğu çalışma çalışanların bilgi güvenliği farkındalığının orta düzeyin üzerinde veya yüksek olduğunu göstermektedir. İlgili alan yazında yer alan bulgular ve teorik bilgiler ışığında çalışanların bilgi güvenliğini izlemeye ve iyileştirmeye yönelik çalışmalar, bilgi güvenliği ve güvenli İnternet kullanımına yönelik gerçekleştirilen eğitimler ve kamu spotları, bilgi güvenliği ihlali durumunda yaşanacak risk faktörlerine yönelik bilgilendirmeler ve yaşanan deneyimlerin (Thomson, Von Solms ve Louw, 2006; Peltier, 2013; Han vd., 2015; Güldüren, 2015; Genç, 2019) kişisel bilgi güvenliği farkındalığının yüksek olmasıyla ilişkili olabileceği düşünülmektedir. Teknolojinin yaygın kullanımı, bilgi güvenliği ihlalleri nedeniyle yaşanan olumsuzluklara ilişkin haberler, bilgi güvenliğine yönelik eğitimler ve

bilgilendirme çalışmaları, kamu kurumlarının bilgi güvenliğine yönelik bilgilendirmeleri gibi çalışmaların kişisel bilgi güvenliği farkındalığının yüksek olmasında etkili olduğu söylenebilir. Bu sonuca göre üniversitede görev yapan akademik ve idari personelin bilgi güvenliği farkındalığının yüksek olması kişisel bilgi güvenliğinin sağlanması açısından olumlu bir durum olarak değerlendirilebilir.

Araştırma sonucunda üniversitede görev yapan akademik ve idari personelin örgütsel iletişim düzeyinin yüksek olduğu belirlenmiştir. Çanak ve Avcı (2016) öğretmenler ile gerçekleştirdikleri çalışmada, katılımcıların örgütsel iletişim düzeyinin "katılıyorum" seviyesinde olduğu sonucuna ulaşmışlardır. Benzer bir çalışmada Ataş Akdemir (2019) öğretmenlerin örgütsel iletişim seviyesinin yüksek olduğunu belirtmiştir. Örgüt içerisindeki iletişimi formel ve informel iletişim olarak inceleyen çalışmalarda da benzer sonuçlara rastlanmıştır. Efeoğlu ve Çetin (2012) belediye çalışanlarıyla gerçekleştirdikleri çalışmada, kurum içerisinde formel ve informel iletişimlerinin iyi düzeyde olduğu sonucuna ulaşmışlardır. Vander Elst, Baillien, De Cuyper ve De Witte (2010) iş güvencesizliği ve örgütsel iletişim arasında olumsuz bir ilişki olduğunu belirtmişlerdir. İlgili alan yazın ve teorik bilgilere göre örgütsel iletişimin olumlu örgüt kültürü, örgütsel bağlılık, örgütsel vatandaşlık, yüksek dinleme becerisi (Robbins ve Judge, 2013; Gochhayat vd., 2017; Guffey ve Loewy, 2021; Ross, 2021) gibi değişkenlerden olumlu etkilendiği belirlenmiştir. Bu bağlamda çalışanların örgütsel iletişiminin yüksek olması, kurum içerisindeki bu faktörlerin etkili olmasıyla ilişkili olabileceği düşünülmektedir. Kurum çalışanlarının ortak çalışma alanlarını veya odaları paylaşması, çalışmanın bir kamu kurumunda gerçekleştirilmesi nedeniyle rekabet ortamının yoğun olmaması, kurum içerisinde birlikte uzun süre çalışan personelin bulunması gibi nedenlerle örgütsel iletişim seviyesinin yüksek olduğu söylenebilir. Üniversitede görev yapan akademik ve idari personelin örgütsel iletişiminin yüksek olması olumlu bir iletişim ortamının bulunması, bilgi ve deneyim aktarılması, etkili iletişimin kurulmasına fırsat tanıması açısından üniversiteler için olumlu bir durum olarak değerlendirilebilir.

Gerçekleştirilen analiz sonucunda üniversitede görev yapan akademik ve idari personelin bilgi paylaşma düzeylerinin yüksek olduğu belirlenmiştir. Alan yazın incelendiğinde benzer sonuçların yer aldığı görülmüştür. Ulusoy (2015), telekomünikasyon sektöründe görev yapan personelle gerçekleştirdiği çalışmada katılımcıların bilgi paylaşım düzeyinin orta düzey olduğunu belirtmiştir. Uludağ, Aktaş ve Özdoğaç Özgit (2019), eğitim çalışanları ile gerçekleştirdikleri çalışmada, katılımcıların bilgi paylaşma algısının yüksek olduğu sonucuna ulaşmışlardır. Kurum içerisinde bilgi paylaşımının sağlanması için ilgili alan yazın ve teorik bilgiler incelendiğinde bilgiyi paylaşmanın kurumu güçlendireceği algısı, bilgi paylaşımın ödüllendirilmesi, kişisel özelliklerin dikkate alınması gibi faktörlerin önemli olduğunu gösteren çalışmalara rastlanmıştır (Bartol ve Srivastava, 2002; Cabrera ve Cabrera, 2005; Matzler ve arkadaşları, 2008; Zawawi vd., 2011; Chen ve Hsieh, 2015). Ayrıca işbirliği, iletişim becerileri, öz yeterlilik, olumlu örgüt kültürü, adalet gibi değişkenlerin bilgi paylaşma ile yakından ilişkili olduğunu gösteren çalışmalar yer almaktadır (Gurteen, 1999; Cabrera ve Cabrera, 2005; Cabrera vd., 2006; Chen ve Hsieh, 2015). Araştırma sonucunda üniversitede görev yapan akademik ve idari personelin bilgi paylaşımının yüksek olması nedeniyle, örgüt içerisinde bilgi paylaşımının desteklenmesine ve bilgi paylaşımını engelleyici durumların ortadan kaldırılmasına yönelik davranışların teşvik edildiği düşünülmektedir. Bu sonuca göre üniversitede görev yapan akademik ve idari personelin bilgi paylaşımının yüksek olması personelin bilgi düzeyinin artması, bilginin tek bir çalışanda toplanmaması, yeni bilginin hızlı uygulanması, bir alanda sahip olunan uzmanlığın farklı alanlarda kullanılabilmesi açısından üniversiteler için olumlu görülecek bir durum olarak değerlendirilebilir.

Araştırma sonucunda elde edilen bulgular ışığında üniversitelerde görev yapan akademik ve idari personelin kurumsal bilgi güvenliği, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşım düzeylerinin yüksek olduğu; bu sonucun üniversiteler için olumlu bir durum olduğu söylenebilir.

5.2. İkinci Araştırma Problemine İlişkin Sonuç ve Tartışma

"Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği farkındalığı, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı cinsiyete, yaşa, hizmet süresine, İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığına göre anlamlı farklılık göstermekte midir?" araştırma sorusuna yönelik gerçekleştirilen analiz sonuçlarına ilişkin bulgular sunulmuştur.

5.2.1. Cinsiyet Değişkenine Göre Farklılık Analizine İlişkin Sonuç ve Tartışma

Analiz sonuçları incelendiğinde katılımcıların kurumsal bilgi güvenliğinin, kişisel bilgi güvenliği farkındalığının, örgütsel iletişimin ve örgütsel bilgi paylaşımının cinsiyete göre anlamlı farklılaşmadığı belirlenmiştir. Bu sonuç cinsiyetin üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliğinin, kişisel bilgi güvenliği farkındalığının, örgütsel iletişimin ve örgütsel bilgi paylaşımı düzeyleri üzerinde bir değişim oluşturmadığını göstermektedir. Alan yazın incelendiğinde araştırma sonucuna benzerlik gösteren çalışmalara rastlanmıştır. Baran ve Şener (2020a), kamu kurumunda çalışan personelin kurumsal bilgi güvenliğinin cinsiyete göre anlamlı farklılık göstermediği sonucuna ulaşmışlardır. Hastane çalışanları ile gerçekleştirdiği çalışmada Gerçeker (2012), kurumsal bilgi güvenliğinin cinsiyete göre anlamlı farklılık göstermediğini belirtmişlerdir. Kadın ve erkek çalışanların kurumsal bilgi güvenliğine yönelik benzer davranışlar göstermesi, güvenlik risklerine yönelik benzer farkındalığa sahip olması, güvenlik önlemlerine yönelik teşvikler, düzenlenen eğitimler gibi nedenlerin kurumsal bilgi güvenliğinin cinsiyete göre farklılaşmamasında etkili olduğu söylenebilir. Ayrıca ilgili literatürde kurumsal bilgi güvenliğine yönelik yapılacak çalışmalarda cinsiyete göre farklılıkların araştırılması önerilmektedir (Safa, Von Solms ve Furnell, 2016). Gerçekleştirilen çalışma ile alan yazına bu bağlamda katkı sağlandığı düşünülebilir.

Özdemir ve Uluyol (2021), kamu kurumunda çalışan personel ile Nezgitli ve Gökçearslan (2022) kamu ve özel sektörde çalışanlarla gerçekleştirdikleri çalışmada bilgi güvenliği farkındalığının cinsiyete göre anlamlı farklılık göstermediği sonucuna ulaşmışlardır. Okul ve arkadaşları (2018), konaklama işletmelerinde çalışan personelle gerçekleştirdikleri çalışmada bilgi güvenliği farkındalığının cinsiyete göre anlamlı farklılaşmadığını belirtmişlerdir. Benzer bir çalışmada kamu hastanesinde çalışan personelin kişisel verilerin korunmasına yönelik görüşlerinin cinsiyete göre anlamlı farklılık göstermediği bulgulanmıştır (Çelik Çöp, 2017). Wiley, McCormac ve Calic (2020) 508 çalışanla gerçekleştirdikleri çalışmada bilgi güvenliği farkındalığının cinsiyete göre anlamlı farklılık göstermediği sonucuna ulaşmıştır. Ünver (2019), insan kaynakları çalışanlarının bilgi güvenliği uygulamalarına yönelik görüşlerinin cinsiyete göre anlamlı farklılık göstermediğini belirtmişlerdir. İlgili alan yazın incelendiği araştırma bulgusundan farklı sonuçların yer aldığı çalışmalara da rastlanmıştır. Alemdaroğlu (2020) bilgi güvenliği farkındalığının erkek çalışanların lehine anlamlı olduğu sonucuna ulaşmıştır. McGill ve Thompson (2018) gerçekleştirdikleri çalışmada benzer bir sonuca ulaşmıştır ve kadınların daha düşük seviyede bilgi güvenliği davranışı sergilediğini bulgulamışlardır. Farklı bir çalışmada ise Anwar ve arkadaşları

(2017) gerçekleştirdiği çalışmada çalışanların bilgisayar ve İnternet güvenliği davranışlarının bilgi güvenliğinin erkekler lehine anlamlı farklılık gösterdiğini belirtmişlerdir. Ancak gerçekleştirdikleri çalışmada anlamlı farklılık olmasına rağmen kadınların siber güvenlik risklerine karşı daha savunmasız olmadığını da vurgulamışlardır. Bu sonuç araştırma bulgusunu destekler niteliktedir. Elde edilen sonuçlar ve alan yazında yer alan çalışmalar ışığında erkek ve kadınların teknoloji kullanma becerilerinin benzer seviyelerde olduğu, benzer düzeyde güvenlik önlemi aldığı, güvenlik olayları sonuçlarına ilişkin algılarının yakın düzeylerde olduğu düşünülebilir.

Araştırma sonucunda katılımcıların örgütsel iletişiminin cinsiyete göre anlamlı farklılaşmadığı belirlenmiştir. İnce ve Gül (2011) ile Topsakaloğlu (2015), kamu kurumunda çalışan personelle gerçekleştirdiği çalışmada örgütsel iletişimin cinsiyete göre anlamlı farklık göstermediği sonucuna ulaşmışlardır. Öğretmenlerle gerçekleştirilen benzer çalışmalarda öğretmenlerin örgütsel iletişime yönelik algılarının cinsiyete göre anlamlı farklılık göstermediği belirlenmiştir (Kurt, 2014; Ertürk ve Aydın, 2018). Yazıcıoğlu (2019) öğretmenler, Tekin (2015) belediye çalışanları ile gerçekleştirdikleri çalışmalarda kurum içi etkin iletişim ortamı algılarının cinsiyete göre anlamlı farklılık göstermediği sonucuna ulaşmıştır. İlgili alan yazın incelendiğinde araştırma sonucundan farklı sonuçlara da ulaşılmıştır. Öğretmen adayları ile gerçekleştirilen çalışmada Kılcıgil, Bilir, Özdinç, Eroğlu ve Eroğlu (2009) kadın öğretmen adaylarının iletişim becerilerinin erkek adaylardan daha iyi düzeyde olduğunu belirtmişlerdir. Benzer bir çalışmada ise Çuhadar, Özgür, Akgün ve Gündüz (2014) kadın öğretmen adaylarının iletişim becerilerinin erkeklerden daha yüksek olduğu sonucuna ulaşmışlardır. Erkek ve kadın çalışanların benzer örgütsel iletişim becerilerine ve seviyesine sahip olması, örgüt içerisinde iletişimin teşvik edilmesi gibi nedenlerle cinsiyete göre anlamlı farklılığın oluşmadığı söylenebilir.

Araştırma sonucunda örgütsel bilgi paylaşımının da cinsiyete göre anlamlı farklılık göstermediği ve ilgili alan yazında benzer sonuçların yer aldığı belirlenmiştir. Baran ve Şener (2020a), örgütsel bilgi paylaşımının cinsiyete göre anlamlı farklılık göstermediğini belirtmişlerdir. Benzer bir çalışmada Uludağ, Aktaş ve Özdoğaç Özgit (2019), eğitim çalışanlarının bilgi paylaşımını inceledikleri çalışmada cinsiyete göre anlamlı farklılık olmadığı sonucuna ulaşmışlardır. Alan yazında araştırma bulgusundan farklı sonuçların yer aldığı çalışmalara da rastlanmıştır. Güngör ve Celep (2016), öğretmenlerle gerçekleştirdikleri çalışmada örgüt içi bilgi paylaşmanın erkek öğretmenler lehine anlamlı farklılık gösterdiği sonucuna ulaşmışlardır. Öneren, Çiftçi ve Harman (2016) mobilya sektöründe çalışan katılımcılarla gerçekleştirdikleri çalışmada erkek çalışanların bilgi paylaşma düzeylerinin kadın çalışanlardan yüksek olduğunu belirtmişlerdir. Nişancı ve Bakkal (2020), erkek çalışanların bilgi paylaşma düzeyinin kadınlardan daha yüksek olduğu sonucuna ulaşmışlardır. Erkek ve kadın çalışanlar açısından kurum içerisindeki bilgi paylaşımının son yıllarda daha fazla teşvik edilmesi, bilgi paylaşmanın örgüte sağladığı faydaların kadın ve erkek çalışanlar tarafından daha fazla önemsenmesi gibi nedenlerle cinsiyete göre anlamlı farklılığın oluşmadığı düşünülmektedir. İlgili alan yazında örgütsel bilgi paylaşımına yönelik yapılacak çalışmalarda cinsiyete göre farklılıkların araştırılması önerilmektedir (Miller ve Karakowsky, 2005; Jiang ve Hu, 2016). Gerçekleştirilen çalışma ile alan yazına bu bağlamda katkı sağlandığı düşünülmektedir.

Araştırma sonucunda cinsiyetin kurumsal bilgi güvenliği, bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşım üzerinde anlamlı bir ayrıma neden olmadığı söylenebilir. Ayrıca elde edilen sonuçla ilgili literatüre bu alanda katkı sağladığı düşünülmektedir.

5.2.2. Yaş Değişkenine Göre Farklılık Analizine İlişkin Sonuç ve Tartışma

Analiz sonuçlarına göre araştırma değişkenlerinden kurumsal bilgi güvenliği ve alt boyutları yaş değişkenine göre anlamlı farklılık göstermemektedir. İlgili alan yazın incelendiğinde çalışma sonucundan farklı çalışmalara rastlanmıştır. Chua, Wong, Low ve Chang (2018) gerçekleştirdikleri çalışmada yaşı daha büyük olan çalışanların bilgi güvenliği politikalarına yönelik daha bilinçli ve uyumlu olduğu sonucuna ulaşmışlardır. Ancak araştırma bulgusuna benzer sonuçların yer aldığı çalışmalara da rastlanmıştır. Gerçeker (2012) kurumsal bilgi güvenliğinin yaş değişkenine göre anlamlı farklılık göstermediğini belirtmiştir. Araştırmada çalışanlar kurumsal bilgi güvenliği düzeylerinin yüksek olması, kurumun varlıklarının öneminin farkında olmaları gibi nedenlerle yaş değişkenine göre anlamlı farklılığın olmadığı söylenebilir.

Araştırma kapsamında elde edilen sonuçlara göre bilgi güvenliği farkındalığı, bilgi güvenliği farkındalığının saldırı ve tehditler boyutu ile kişisel verilerin korunması boyutları yaş değişkeni açısından anlamlı farklılık gösterdiği belirlenmiştir. Bilgi güvenliği farkındalığı, saldırı ve tehditler ile kişisel verilerin korunması alt boyutu 35 yaş altı olan katılımcıların lehine anlamlı farklılık göstermektedir. İlgili alan yazın incelendiğinde benzer sonuçlara rastlanmıştır. Aslan Öztezcan (2017), üniversitelerde akademik ve idari personel üzerinde gerçekleştirdiği çalışmada kişisel verilerin korunması ile saldırı ve tehditler boyutunun yaşa göre anlamlı farklılık gösterdiğini ve bu farkın genç katılımcıların lehine olduğu sonucuna ulaşmışlardır. Benzer bir çalışmada kamu çalışanlarının bilgi güvenliği kültürünün yaşa göre anlamlı farklılık gösterdiği ve daha genç katılımcıların bilgi güvenliği kültürü ortalamalarının daha yüksek olduğu belirlenmiştir (Baran ve Şener, 2020b). Wiley, McCormac ve Calic (2020) gerçekleştirdikleri çalışmada bilgi güvenliği farkındalığının yaşa göre anlamlı farklılık gösterdiğini ve anlamlı farklılığın 30 yaş altı katılımcıların lehine olduğu sonucuna ulaşmışlardır. Özdemir ve Uluyol (2021), kamu kurumunda çalışan personelin bilgi güvenliğinin 31-40 yaş aralığındaki katılımcıların lehine anlamlı farklılık gösterdiği sonucuna ulaşmışlardır. Ancak alan yazın incelendiğinde araştırma sonucunu desteklemeyen çalışmalara da rastlanmıştır. Alemdaroğlu (2020) bankacılık sektöründe çalışan personelin bilgi güvenliği farkındalığının yaşa göre anlamlı farklılık göstermediği sonucuna ulaşmıştır. Araştırma sonucuna göre üniversitede görev yapan akademik ve idari personelden daha genç yaşta olan katılımcıların bilgi güvenliği farkındalığı ile saldırı ve tehditler konusunda daha fazla farkındalığa sahip olduğu söylenebilir. Genç çalışanların teknolojiyi daha yaygın kullanması ve bu nedenle risklere daha fazla aşina olmaları gibi nedenlerin bilgi güvenliği farkındalığının daha genç katılımcılar lehine anlamlı farklılık göstermesiyle ilişkili olduğu düşünülebilir.

Araştırma sonucunda örgütsel iletişim ve örgütsel iletişimin formel iletişim alt boyutu yaş değişkenine göre anlamlı farklılık göstermemektedir. Alan yazın incelendiğinde benzer sonuçlara rastlanmıştır. Ertürk ve Aydın (2018), öğretmenlerin örgütsel iletişime yönelik algılarının yaş değişkenine göre anlamlı farklılık göstermediğini belirtmişlerdir. Benzer bir çalışmada Kurt (2014) ve Bulut (2019) örgütsel iletişimin yaş değişkenine göre anlamlı farklılık göstermediği sonucuna ulaşmıştır. Yazıcıoğlu (2019), öğretmenlerin kurum içi etkin iletişim ortamı algılarının yaşa göre anlamlı farklılık göstermediği sonucuna ulaşmıştır. Tekin (2015) belediye çalışanları ile gerçekleştirdikleri çalışmalarda kurum içi etkin iletişim ortamı algılarının yaşa göre anlamlı farklılık göstermediği sonucuna ulaşmıştır. Ayrıca ilgili alan yazında araştırma sonucundan farklı sonuçlara da rastlanmıştır. Günbayı (2007), öğretmenlerle gerçekleştirdiği çalışmada yaşlı öğretmenlerin örgütsel iletişimin etkinliğinde gençlerden daha yüksek puan aldığı sonucuna ulaşmıştır. Aghedr (2021) gerçekleştirdiği çalışmada ise 45 yaş ve üzeri katılımcıların lehine

anlamlı farklılık olduğunu belirtmiştir. Araştırma sonucundan yola çıkarak örgüt içerisindeki her yaş grubundaki çalışanların örgütsel iletişim ile formel iletişim konusunda duyarlı olduğu ve örgütsel iletişim kanallarını kullandığı söylenebilir. Ayrıca bu çalışmanın örneklemini bir kamu kurumu oluşturması nedeniyle her yaş grubundan çalışanların resmi (formel) iletişim kanallarını kullanma konusunda duyarlı olduğu düşünülebilir.

Örgütsel iletişim ölçeğinin informel iletişim boyutu yaş değişkenine göre anlamlı farklılık göstermektedir ve bu farklılık 35 yaş altı katılımcıların lehinedir. Benzer bir çalışmada Arslan ve Afat (2019), informel iletişimin yaşa göre anlamlı farklılık gösterdiğini ve bu farkın 26-30 yaş grubunda olan katılımcıların lehine olduğu sonucuna ulaşmışlardır. Koch ve Denner (2022), yaşın informel iletişimin güçlü bir yordayıcısı olduğunu ve genç yaştaki katılımcıların informel iletişimi daha fazla kullandıklarını belirtmişlerdir. Todisco, Tomo, Canonico, Mangia ve Sarnacchiaro (2021) gerçekleştirdikleri çalışmada genç kamu çalışanlarının sosyal medyayı kamunun karar alma süreçlerinde yararlı olarak gördüğünü belirtmişlerdir. Auxier ve Anderson (2021) 18-29 yaş arasındaki katılımcıların %71'nin Instagramı, %65'nin Snapchatı kullandığını ve bu sosyal medya sitelerinin genç yetişkinler arasında güçlü takipçi kitlesinin olduğunu belirtmişlerdir. Benzer bir çalışmada ise Oksa, Kaakinen, Savela, Ellonen ve Oksanen (2020) sosyal medyanın kurumun hedeflerine ulaşmak için kullanılabileceğini, bunun örgüt içerisindeki informel iletişim olduğunu vurgulamışlardır. Bu bağlamda genç katılımcıların sosyal medyayı kullanmaları ve bu durumu kamu çalışmaları içinde faydalı görmeleri, informel iletişim konusunda daha hassas olmaları gibi nedenlerle informel iletişimin daha genç çalışanlar lehine anlamlı farklılık gösterdiği düşünülebilir.

Üniversitede görev yapan akademik ve idari personelin genel bilgi paylaşımı, açık ve örtük bilgi paylaşımı alt boyutları yaş değişkenine göre anlamlı farklılık göstermektedir ve bu farklılık 35 yaş altı katılımcıların lehinedir. Alan yazın incelendiğinde araştırma sonucuna benzer sonuçlara rastlanmıştır. Altındiş ve Ağca (2011) gerçekleştirdikleri çalışmada sağlık çalışanlarından 18-25 yaş aralığında olan katılımcıların bilgi paylaşım engellerini daha az algıladıkları sonucuna ulaşmışlardır. Benzer bir çalışmada işgücüne yeni giren genç çalışanların, bilgi paylaşımı ve iletişim için sosyal medyayı ve teknolojiyi kullandığı belirtilmiştir (Jarrahi, 2017). Ancak araştırma sonucundan farklı sonuçların yer aldığı araştırmalara da rastlanmıştır. Aghedr (2021) gerçekleştirdiği çalışmada bilgi paylaşımının yaş değişkenine göre anlamlı farklılık gösterdiği ve bu farkın 45 yaş ve üzeri olan katılımcıların lehine olduğunu; Öneren, Çiftçi ve Harman (2016) mobilya sektöründe çalışan katılımcılarla gerçekleştirdikleri çalışmada 18-24 yaş arası katılımcıların çalışanlar arası bilgi paylaşım algı düzeyinin daha düşük olduğunu belirtmişlerdir. Nişancı ve Bakkal (2020) ise yaşa göre anlamlı farklılık olmadığı sonucuna ulaşmışlardır. Alan yazında farklı sonuçlar olmasına rağmen gençlerin teknolojiyi ve sosyal medyayı daha sık kullanmaları bilgi paylaşımının daha genç katılımcılar lehine anlamlı farklılık göstermesi ile ilişkili olabilir. Araştırma sonucunda daha genç katılımcıların, açık ve örtük bilgi paylaşımı konusunda daha fazla duyarlı oldukları söylenebilir.

5.2.3. Hizmet Süresi Değişkenine Göre Farklılık Analizine İlişkin Sonuç ve Tartışma

Analiz sonuçlarına göre araştırma değişkenlerinden kurumsal bilgi güvenliği ve alt boyutlarının hizmet süresi değişkenine göre anlamlı farklılık göstermediği belirlenmiştir. Katılımcıların kurumsal bilgi güvenliğine yönelik algılarının ve duyarlılıklarının benzer olması

nedeniyle kurumsal bilgi güvenliğinin hizmet süresine göre anlamlı farklılık göstermediği söylenebilir.

Hizmet süresine değişkenine göre genel bilgi güvenliği farkındalığı, saldırı ve tehditler ile kişisel verilerin korunması alt boyutları 5 yıldan az olan katılımcıların lehine anlamlı farklılık göstermektedir. Benzer bir çalışmada bilgi güvenliği kültürünün çalışma süresine göre anlamlı farklılık gösterdiği ve bu sonucun 1-5 yıl çalışanların lehine olduğu belirlenmiştir (Baran ve Şener, 2020b). Khan, Ibrahim ve Hussain (2021), kütüphane personeli ile gerçekleştirdikleri çalışmada, katılımcıların bilgi güvenliği farkındalığının hizmet süresine göre farklılık gösterdiği ve bu farklılığın 5 yıldan az hizmet süresine sahip katılımcıların lehine olduğu sonucuna ulaşmışlardır. Hizmet süresi az olan katılımcıların yaşlarının daha genç olduğu bu bağlamda da genç çalışanların teknolojiyi yaygın kullanması, bilgi güvenliği ihlallerine aşina olmaları nedeniyle bilgi güvenliği farkındalığı, saldırı ve tehditler, kişisel verilerin korunması alt boyutlarının hizmet süresi az olan katılımcıların lehine anlamlı farklılık gösterdiği düşünülebilir. Bu sonuçlardan yola çıkarak hizmet süresi daha az olan katılımcıların bilgi güvenliği farkındalığı, saldırı ve tehditler, kişisel verilerin korunması konusunda daha hassas olduğu söylenebilir.

Analiz sonuçlarına göre örgütsel iletişim ve örgütsel iletişimin formel iletişim alt boyutunun hizmet süresi değişkenine göre anlamlı farklılık göstermediği belirlenmiştir. Ertürk ve Aydın (2018), öğretmenlerle gerçekleştirdiği çalışmada benzer bir sonuca ulaşmıştır ve öğretmenlerin örgütsel iletişime yönelik algılarının hizmet süresi değişkenine göre anlamlı farklılık göstermediğini belirtmişlerdir. Benzer bir çalışmada Kurt (2014) örgütsel iletişimin mesleki deneyime göre anlamlı farklılık göstermediği sonucuna ulaşmıştır. Yazıcıoğlu (2019), öğretmenlerin kurum içi etkin iletişim ortamı algılarının mesleki deneyime göre anlamlı farklılık göstermediği sonucuna ulaşmıştır. Tekin (2015) belediye çalışanları ile gerçekleştirdiği çalışmada kurum içi etkin iletişim ortamı algılarının çalışma süresine göre anlamlı farklılık göstermediğini belirtmiştir. Araştırma sonucundan farklı olarak Çanak ve Avcı (2016), örgütsel iletişimin kurumda çalışma süresine göre yapılan analiz sonucunda anlamlı farklılığın daha az süre çalışanların lehine olduğu sonucuna ulaşmışlardır. Araştırma sonucundan yola çıkarak örgüt içerisindeki farklı mesleki deneyimi olan çalışanların benzer iletişim becerilerine ve örgütsel iletişime yönelik olumlu algılara sahip olduğu düşünülebilir. Aynı zamanda çalışmanın bir kamu kurumunda gerçekleştirilmesi nedeniyle farklı deneyimi olan çalışanların formel iletişim kanallarını kullanma açısından hassas olduğu söylenebilir.

Örgütsel iletişimin informel iletişim boyutu hizmet süresine göre anlamlı farklılık göstermektedir ve bu fark 5-10 yıl olan katılımcıların lehinedir. Aynı zamanda örgütsel bilgi paylaşımı, açık ve örtük bilgi paylaşımı alt boyutları hizmet süresine göre anlamlı farklılık göstermektedir ve bu farklılık hizmet süresi 5 yıldan az olan katılımcıların lehinedir. Alan yazın incelendiğinde araştırma bulgusundan farklı sonuçlara da rastlanmıştır. Aghedr (2021) bilgi paylaşımının mesleki deneyimi 15 yıl ve üzeri katılımcıların lehine anlamlı farklılık gösterdiği sonucuna ulaşmıştır. Güngör ve Celep (2016) mesleki kıdemi fazla olan öğretmenlerin örgüt içi bilgi paylaşma düzeylerinin daha yüksek olduğunu belirtmişlerdir. Ancak araştırma sonucundan yola çıkarak hizmet süresi daha az olan katılımcıların örgütsel bilgi paylaşımı, açık ve örtük bilgi paylaşımı, informel iletişim konusunda daha duyarlı olduğu söylenebilir.

5.2.4. İnternette/Sosyal Ağ Sitelerinde Gizlilik/Güvenlik Ayarlarını Kontrol Etme Sıklığına Göre Farklılık Analizine İlişkin Sonuç ve Tartışma

Kurumsal bilgi güvenliği ölçeğinin bilgi güvenliğinde gizlilik alt boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermemektedir. Ancak analiz sonuçlarına göre kurumsal bilgi güvenliği, bilgi güvenliği kültürü ve bilgi güvenliği yönetimi boyutları İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını ayda birkaç defa ve ayda bir defa kontrol eden katılımcıların lehine anlamlı farklılık göstermektedir. Bilgi güvenliği uygulaması, bilgi güvenliği yaklaşımı boyutları ise İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını ayda bir defa kontrol eden katılımcıların lehine anlamlı farklılık göstermektedir. İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme durumu kişisel bilgi güvenliği farkındalığı ile yakından ilişkili olduğu düşünülmektedir. İlgili alan yazın (Al-Omari, El-Gayar ve Deokar, 2012; Ahlan, Lubis ve Lubis, 2015; Da Veiga ve arkadaşları, 2020) ve bu araştırma sonucunda kişisel bilgi güvenliği farkındalığı ile kurumsal bilgi güvenliği arasında pozitif yönlü bir ilişki olduğunu göstermektedir. Aynı zamanda bilgi güvenliğinin sağlanmasında temel faktörler arasında yer alan yetkisiz erişimin engellenmesi için gizlilik/güvenlik ayarlarının sık kontrol edilmesinin faydalı olacağı söylenebilir. Bu nedenle kurumsal bilgi güvenliği, bilgi güvenliği kültürü, bilgi güvenliği yönetimi, bilgi güvenliği yaklaşımı boyutlarının İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını sık kontrol eden katılımcıların lehine anlamlı farklılık gösterdiği düşünülmektedir.

Bilgi güvenliği farkındalığı ve kişisel verilerin korunması boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığına göre anlamlı farklılık göstermektedir. Analiz sonuçlarına göre bu fark ayda birkaç defa, ayda bir defa ve yılda birkaç defa yanıtını veren katılımcıların lehinedir. Bilgi güvenliğinin saldırı ve tehditler boyutu ise İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını ayda birkaç defa ve yılda birkaç defa kontrol eden katılımcıların lehine anlamlı farklılık göstermektedir. Mamonov ve Benbunana-Fich (2018) gerçekleştirdiği çalışmada güçlü şifre seçimi ile bilgi güvenliği tehditlerinin farkında olunması arasında pozitif bir ilişki olduğunu belirtmiştir. Liu, Tse, Kwok ve Chiu (2022) gerçekleştirdikleri çalışmada gizlilik koruması konusunda farkındalığı olan kişilerin bile şifrelerini periyodik olarak değiştirmediği sonucuna ulaşmışlardır. Aynı çalışmada bazı kamu kurumlarının çalışanlarının periyodik olarak şifrelerini güncellemelerini talep ettiğini ve bu durumun sosyal medya şifrelerini güncellemeyi de hatırlattığını belirtmişlerdir. Bu araştırmanın bir kamu kurumunda çalışan personellerle gerçekleştirilmesi nedeniyle İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını sık kontrol eden katılımcıların bilgi güvenliği farkındalığı, saldırı ve tehditler ile kişisel verilerin korunmasında hassas olduğu söylenebilir.

Örgütsel iletişim ve formel iletişim alt boyutu, bilgi paylaşımının açık bilgi paylaşım alt boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını kontrol etme sıklığı değişkenine göre anlamlı farklılık göstermemektedir. Örgütsel iletişimin informel iletişim boyutu İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını ayda birkaç defa kontrol eden katılımcıların lehine anlamlı farklılık göstermektedir. Analiz sonuçlarına göre bilgi paylaşımı İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını ayda birkaç defa ve ayda bir defa kontrol eden katılımcıların lehine anlamlı farklılık göstermektedir. Bilgi paylaşımının örtük bilgi paylaşımı boyutu ise İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını ayda birkaç defa kontrol eden katılımcıların lehine anlamlı farklılık göstermektedir. Çalışanlar sosyal medya ve İnternet ortamıyla güçlü ilişkiler kurmakta, sosyal medya ile informel ağlar ve ilişkiler artmakta böylelikle hem

çalışana hem kuruma fayda sağlanabilmektedir. Bu nedenle çalışanlar sosyal medya ve İnternet ortamını yaygın bir biçimde kullanmaktadır (Jarrahi, 2017). Sosyal medya siteleri informel iletişime ve örtük bilgi paylaşmaya imkan tanımaktadır. Bu bağlamdan yola çıkarak İnternette/sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını sık kontrol eden katılımcıların informel iletişim ve örtük bilgi paylaşma konusunda daha duyarlı olduğu söylenebilir.

5.3. Üçüncü Araştırma Problemine İlişkin Sonuç ve Tartışma

Bu başlıkta "Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliği ile kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı arasında bir ilişki var mıdır?" alt amaca yönelik sonuç ve tartışmalar yer almaktadır.

Araştırma sorusuna yanıt aramak için korelasyon, regresyon ve yol analizi gerçekleştirilmiştir. Korelasyon analizi sonucunda kurumsal bilgi güvenliği ile saldırı ve tehditler, kişisel verilerin korunması, formel iletişim, informel iletişim, açık bilgi paylaşımı ve örtük bilgi paylaşımı arasında pozitif yönlü orta düzey anlamlı bir ilişki olduğu belirlenmiştir.

Araştırma sorusuna yanıt aramak için gerçekleştirilen regresyon analizi sonucuna göre saldırı ve tehditler, kişisel verilerin korunması, formel iletişim, örtük bilgi paylaşımının kurumsal bilgi güvenliğinin anlamlı yordayıcısı olduğu belirlenmiştir. Ayrıca ilgili literatür ve yapılan araştırmalar temel alınarak geliştirilen model, yapısal eşitlik modellemesi ile test edilmiş ve modelin uyum değerlerinin kabul edilebilir ve mükemmel uyum gösterdiği belirlenmiştir. Yapılan yol analizi sonucunda, saldırı ve tehditler, kişisel verilerin korunması, formel iletişim kurumsal bilgi güvenliğini doğrudan ve pozitif yönde etkilemektedir.

"Saldırı ve tehditlere yönelik farkındalık ile kişisel verilerin korunmasına yönelik farkındalık kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkiler" (H1 ve H2) hipotezleri kabul edilmiştir. Bu sonuca göre kişisel bilgi güvenliği farkındalığına sahip kişilerin kurumsal bilgi güvenliğine de sahip olduğu söylenebilir. İlgili alan yazın incelendiğinde Ahlan, Lubis ve Lubis (2015), üniversitede çalışan katılımcılarla gerçekleştirdiği çalışmada, bilgi güvenliği önlemlerini takip etme ve uygulama konusunda olumlu tutum ve öz yeterliliğe sahip olma durumunun kurumsal bilgi güvenliği farkındalığını pozitif yönde olumlu etkilediği sonucuna ulaşmışlardır. Al-Omari, El-Gayar ve Deokar (2012), dokuz finans örgütü çalışanları ile yaptığı çalışmada, çalışanların bilgi güvenliği farkındalığının bilgi güvenliği politikalarının gereksinimlerine uygun davranmalarını pozitif yönde etkilemektedir. Benzer bir çalışmada bilgi güvenliği tehditlerinin farkında olunması bilgi güvenliğine yönelik davranışlar (güçlü şifre seçimi, kişisel bilgilerin paylaşılmaması) gösterilmesi üzerinde olumlu etkisi olduğunu belirtmiştir (Mamonov ve Benbunana-Fich, 2018). Da Veiga ve arkadaşları (2020), sanayi kuruluşlarında çalışan personelin kurumsal bilgi güvenliğini etkileyen faktörleri inceledikleri çalışmada, bilgi güvenliği bilgisinin kurumsal bilgi güvenliğini etkilediğini belirlemişlerdir. Bulgurcu vd. (2010), gerçekleştirdiği çalışmada çalışanların genel bilgi güvenliği farkındalığının kurumsal bilgi güvenliği politikalarına uyma davranışını doğrudan ve dolaylı olarak etkilediği sonucuna ulaşmışlardır. Çalışanların kurumun bilgi güvenliği politikalarına uymaya yönelik tutumu, inançları, öz yeterliliği kurumun bilgi güvenliği politikalarının gereksinimlerine uyma niyetini olumlu etkilediğini belirtmişlerdir (Bulgurcu vd., 2010).

Çalışanların bilgi güvenliği politikalarına uyumlu davranış sergilemesi kurumsal bilgi güvenliğini olumlu etkileyebilmekte ve aynı zamanda kişisel bilgi güvenliği farkındalığı ile yakından ilişkilidir. Siponen, Pahnila ve Mahmood (2010), bilgi güvenliği politikalarına uyma

davranışı ile inançları, öz yeterliliği, bilgi güvenirliği farkındalık çalışmaları arasında pozitif bir ilişki olduğunu belirlemişlerdir. François (2016), doktora tez çalışmasında bilgi güvenliği politikası farkındalığı ile bilgi güvenliği programının etkinliğiyle arasında pozitif yönde anlamlı bir ilişki olduğu sonucuna ulaşmıştır. Li ve arkadaşları (2019), farklı firmalarda çalışan 579 kişiyle gerçekleştirdiği çalışmada çalışanların bilgi güvenliği politikası farkındalığının, bilgi güvenliği koruma davranışını etkilediği sonucuna ulaşmışlardır. Fakeh, Zulhemay, Shahibi ve Zaini (2012) kütüphanede çalışan personelle gerçekleştirdikleri çalışmada, örgüt içerisinde bilgi güvenliğini güvenlik politikalarının, bilgi güvenliği eğitiminin, teknolojiye yönelik bilginin ve çalışanların davranışlarının etkilediğini belirlemişlerdir.

Ayrıca Rezgui ve Marks (2008), üniversitede görev yapan personelin bilgi güvenliği farkındalığını etkileyen faktörleri araştırdığı çalışmasında, vicdanlılık, kültür, inançlar ve sosyal faktörlerin bilgi güvenliğini etkilediğini ortaya çıkartmışlardır. Benzer bir çalışmada McCormac ve arkadaşları (2017) ise vicdanlılık, uyumluluk, duygusal istikrar, açıklık ve risk alma eğiliminin bilgi güvenliği farkındalığının büyük ölçüde açıkladığı sonucuna ulaşmışlardır. Wiley, McCormac ve Calic (2020) güvenlik kültürü, örgüt kültürü ve bilgi güvenliği farkındalığı arasında pozitif yönlü bir ilişki olduğunu belirtmişlerdir. Hwang, Wakefield, Kim ve Kim, (2019) bilgi güvenliği farkındalığı güvenlik eğitimi, güvenlik politikası, görünürlüğü ve bilgi güvenliği yönetimine katılımın bilgi güvenliğini etkilediği sonucuna ulaşmışlardır. Eminağaoğlu, Uçar ve Eren (2009) bilgi güvenliği farkındalığına yönelik eğitimlerin kurumların bilgi güvenliğini sağlamada güçlü mekanizmalar arasında yer aldığını bulgulamışlardır.

Araştırma sonucunda elde edilen bulgular ışığında, saldırı ve tehditler, kişisel verilerin korunması yani kişisel bilgi güvenliği farkındalığının kurumsal bilgi güvenliğini olumlu yönde etkilediği söylenebilir. Kişisel bilgi güvenliği tehditleri hakkında bilgi sahip olan veya tedbir alan kişilerin, kurumsal bilgi güvenliği hakkında da bilgi sahibi olacağı veya tedbir alacağı ve bu durumun kurumsal bilgi güvenliğine olumlu katkısı olacağı düşünülmektedir. Kurumsal bilgi güvenliğinin sağlanmasında kişisel bilgi güvenliği farkındalığının dikkate alınması gereken faktörler arasında yer almaktadır. Bu noktadan yola çıkarak üniversitelerde görev yapan akademik ve idari personelin kişisel bilgi güvenliği farkındalığını arttırmaya yönelik çalışmaların yapılması kurumsal bilgi güvenliğinin sağlanmasında olumlu katkıda bulunacağı düşünülmektedir. Aynı zamanda alan yazında yer alan çalışmalar ışığında kişisel bilgi güvenliğini etkileyen örgüt kültürü, güvenlik kültürü, vicdanlılık, kültür, inanç, risk alma eğilimi, uyumluluk, duygusal istikrar, açıklık, güvenlik politikası, bilgi güvenliği yönetimine katılım, eğitim gibi faktörlerin kurumsal bilgi güvenliği ile ilgili olabileceği, bu faktörlere yönelik yapılacak çalışmaların kurumsal bilgi güvenliği ile ilişkili olabileceği düşünülmektedir.

Araştırma sonucunda formel iletişimin kurumsal bilgi güvenliğini pozitif yönde olumlu etkilediği sonucuna ulaşılmıştır (H3). İlgili alan yazın incelendiğinde benzer çalışmalara rastlanmıştır. Rezgui ve Marks (2008) üniversitede çalışan personelle gerçekleştirdiği çalışmada, çalışanların bilgi güvenliği farkındalığının düşük olduğunu ve bunun nedenin ise örgüt içerisindeki iletişim yetersizliği olduğunu belirtmiştir. Kraemer ve arkadaşları (2009) ağ yöneticisi ve güvenlik yöneticilerinin insan hatası ile insan ve organizasyon faktörleri hakkındaki görüşleri üzerine yaptığı çalışma sonucunda kurum içerisindeki yeterli olmayan ve tutarsız olan iletişimin kurumsal bilgi güvenliğini olumsuz etkilediğini vurgulamışlardır. Benzer bir çalışmada Arhin ve Wiredu (2018) gerçekleştirdikleri nitel araştırma sonucunda örgüt içerisindeki iletişimin, kurum içerisinde bilgi güvenliği ihlallerinin önlenmesine ve tepki verilmesine olumlu katkı sağladığı sonucuna ulaşmışlardır. Albrechtsen ve Hovden (2010) gerçekleştirdikleri deneysel çalışmada, resmi

sunumlar, e-postalar, çalıştay, grup tartışmaları, sunumlar gibi etkinlikler düzenlemenin yani örgütsel iletişim faaliyetleri gerçekleştirmenin bilgi güvenliği farkındalığını olumlu etkilediğini bu durumunda kurumsal bilgi güvenliğine katkı sağladığını belirtmişlerdir. Benzer bir çalışmada Özdemir-Güngör, Kıdak ve Ercan (2018) hastane personelinin bilgi ihtiyaçlarını karşılamada formel iletişim kanallarının yeterli kabul edildiği sonucuna ulaşmışlardır. Bu sonuçlardan yola çıkarak formel iletişimin kurumsal bilgi güvenliğini ile ilgili bilgilerin çalışanlara iletiminde de kullanılabileceği düşünülmektedir. İlgili alan yazın ve araştırma sonucunda elde edilen bulgular ışığında formel iletişimin kurumsal bilgi güvenliğini olumlu etkilediği ve kurumsal bilgi güvenliğinin sağlanmasında dikkate alınması gerektiği söylenebilir. Örgüt içerisindeki formel iletişimin teşvik edilmesinin kurumsal bilgi güvenliğinin sağlanmasını olumlu etkileyeceği düşünülmektedir.

Postmes, Tanis ve de Wit (2001) gerçekleştirdikleri çalışmada formel iletişimin bir türü olan dikey iletişim ile örgüt bağlılığı arasında güçlü bir şekilde ilişkili olduğu sonucuna ulaşmışlardır. Benzer bir çalışmada formel iletişim ve örgütsel bağlılık arasında pozitif bir ilişki olduğu belirlenmiştir (Lee ve Kim, 2010). İlgili alan yazın incelendiğinde kurumsal bilgi güvenliği politikalarına uyma davranışı ile örgütsel bağlılık arasında pozitif yönlü bir ilişki olduğunu gösteren çalışmalar yer almaktadır (Liu, Wang ve Liang, 2020). Aynı zamanda literatürde yer alan teorik bilgilerde bilgi güvenliğinin sağlanmasında karşılan en büyük sorunlardan birinin bağlılık eksikliği olduğunu göstermektedir (Thomson, Von Solms ve Louw, 2006: 7). Bu noktadan yola çıkarak kurumlar bilgi güvenliğini sağlamak amacıyla kurum içerisinde formel iletişimi ve örgütsel bağlılığı destekleyebilecekleri düşünülmektedir.

Alan yazın incelendiğinde örgütsel iletişim ile örgütsel kültür, liderlik tarzı, örgütsel bağlılık gibi değişkenlerle aynı zamanda kurumsal bilgi güvenliğinin de bu değişkenlerle yakından ilişkili olduğunu bulgulayan çalışmalar yer almaktadır. Örneğin Gochhayat vd., (2017) gerçekleştirdikleri çalışmada, örgüt kültürü ile örgütsel iletişim arasında pozitif yönde anlamlı bir ilişki olduğu sonucuna ulaşmışlardır. Ernest Chang ve Lin (2007) gerçekleştirdikleri çalışmada örgütsel kültür ve bilgi güvenliği arasında anlamlı ilişki olduğunu belirtmişlerdir. Benzer bir çalışmada Tang, Li ve Zhang (2016) örgüt kültürünün kurumun bilgi güvenliği kültürünü etkilediği sonucuna ulaşmışlardır. Benzer şekilde ilgili araştırmalar liderlik tarzı ile bilgi güvenliği (Bhattacharya, 2008) ve liderlik tarzı ile örgütsel iletişimin (Men, 2014;Rocha Flores ve Ekstedt, 2016; Wang ve Xu, 2021) ilişkili olduğunu bulgulayan çalışmalar yer almaktadır. İlgili araştırmalar sonucunda örgütsel iletişimin örgüt kültürü, liderlik tarzı gibi değişkenlerle ilişkili olduğu belirlenmiştir. Bu bağlamda örgütsel iletişim ile yakından ilişki olan bu değişkenlerin kurumsal bilgi güvenliği ile de ilişkili olabileceği, bu değişkenlerin olumlu gelişimine katkı sunulmasının kurumsal bilgi güvenliğinin sağlanmasında faydalı olabileceği söylenebilir. Aynı zamanda açık bilgi paylaşımı ve örtük bilgi paylaşımı ile formel iletişimi ve informel iletişim arasında pozitif yönlü anlamlı bir ilişki olması nedeniyle örgütsel iletişimle yakından ilişkili olan bu değişkenlerin örgütsel bilgi paylaşımına da olumlu katkı sağlayabileceği düşünülmektedir.

Ayrıca alan yazında yer alan çalışmaların genel olarak örgütsel iletişime odaklanmış olmasına rağmen bu çalışmada formel ve informel iletişim olarak daha derin ve detaylı bir inceleme gerçekleştirilerek alana katkı sunduğu söylenebilir.

Araştırma sonucunda informel iletişimin kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkilemediği belirlenmiştir (H4). Rader, Wash ve Brooks (2012) gerçekleştirdikleri nitel çalışmada katılımcıların informel yollarla elde ettikleri bilgi güvenliği bilgilerinin davranışlarını etkilediği sonucuna ulaşmışlardır. Rader ve Wash (2015) gerçekleştirdikleri çalışmada informel

kaynakların bilgi güvenliğine katkı sağlayacağını belirtmişlerdir. Ancak araştırma bulgusu, teorik ve nitel araştırma sonucunda elde edilen bilgiyi desteklememektedir. Bu sonuca göre informel iletişimin kurumsal bilgi güvenliğini sağlamada etkili değişkenler arasında olmadığı söylenebilir. İnformel iletişim ortamlarında kurumun bilgi güvenliği ile ilgili gizli bilgilerin paylaşılabilmesi veya bilgisayarların kullanılabilmesi gibi durumlar kurumsal bilgi güvenliğini olumsuz etkileyebilir. Ancak bilgi güvenliği ile ilgili deneyimler, olumlu katkı sağlayabilecek bilgiler de paylaşılarak kurumsal bilgi güvenliğine olumlu katkı sağlanabilir. İnformel iletişimin böyle bir ikilem oluşturabilmesi nedeniyle informel iletişimin kurumsal bilgi güvenliğini etkilemediği düşünülebilir.

Araştırma sonucunda açık ve örtük bilgi paylaşımının kurumsal bilgi güvenliği düzeyini pozitif ve anlamlı etkilemediği belirlenmiştir (H5, H6). Alan yazın incelendiğinde araştırma bulgusundan farklı sonuçlara rastlanmıştır. Sari ve Prasetio (2017) bilgi paylaşımının bilgi güvenliği farkındalığını etkilediği sonucuna ulaşmışlardır. Araştırma sonucuna göre kurumsal bilgi güvenliğinin sağlanmasında açık ve örtük bilgi paylaşımının etkili olmadığı söylenebilir. İnformel iletişimde olduğu gibi açık ve örtük bilgi paylaşımının kurumsal bilgi güvenliği ile ilgili bir ikilem meydana getirmesi yani bilgiyi paylaşma ve bilgiyi korumanın bir kararsızlık durumu oluşturmasının bu sonuçta etkili olduğu düşünülmektedir. Ayrıca bu araştırmada bilgi paylaşımı örtük ve açık bilgi paylaşımı olarak derinlemesine incelenmiştir. Bu yönden alana katkı sağladığı düşünülmektedir.

Açık bilgi paylaşımı ve örtük bilgi paylaşımı, formel iletişimi ve informel iletişimi doğrudan ve pozitif yönde etkilemektedir (H7, H8, H9, H10). İlgili alan yazın incelendiğinde bilgi paylaşımı ve örgütsel iletişime yönelik benzer sonuçlar yer almaktadır. Affandie, Sulistiyono, Mayasari, Suyono ve Elisabeth (2020) özel bir firmada çalışan personelle gerçekleştirdikleri çalışmada, örgütsel iletişimin bilgi paylaşma üzerinde anlamlı pozitif etkiye sahip olduğu sonucuna ulaşmışlardır. Benzer bir çalışmada, yapıcı bir iletişim ortamının kuruluş içerisindeki bilgi paylaşımı üzerinde olumlu etkisi olduğu belirlenmiştir (Van Den Hooff ve De Ridder, 2004). Razmerita, Kirchner ve Nielsen (2016) kurum içerisindeki bilgi paylaşımını etkileyen faktörleri nitel araştırma yöntemi ile inceledikleri çalışmalarında kurumsal sosyal medya platformlarının kullanımının bilgi paylaşımını olumlu yönde etkilediğini ve kurum içerisinde iletişimin teşvik edilmesi gerektiğini vurgulamışlardır. Gumus (2007) üniversitelerde çalışan personelle gerçekleştirdiği çalışmada bilgi paylaşımı ve iletişim memnuniyeti ile iletişim tarzı arasında güçlü bir ilişki olduğu sonucuna ulaşmıştır.

Ayrıca ilgili alan yazında bilgi paylaşımını açık bilgi paylaşımı ve örtük bilgi paylaşımı, örgütsel iletişimi ise formel iletişim ve informel iletişim olarak araştıran çalışmalara da rastlanmıştır. Hwang (2020) örtük bilgi paylaşımının örgüt içerisindeki çalışanların etkileşimleri diğer bir deyişle iletişimleri ile sınırlı olduğunu belirtmiştir. Ayrıca örgüt içerisindeki bu etkileşim örgütsel çevre ve örgütün özellikleri ile yakından ilişkilidir (Hwang, 2020). Sheerin, Hughes ve Garavan (2020) kadın yöneticilerin örtük bilgi paylaşımını etkileyen faktörleri incelediği çalışmada, örgütsel iletişimin örtük bilgi paylaşımını etkilediği sonucuna ulaşmışlardır. Wijetunge (2012) üniversite kütüphanelerinde çalışan personelle gerçekleştirdiği çalışmada kurum içerisindeki çalışanların veya emekli personellerin kurum içerisinde hikayeler anlatmasının örtük bilgi paylaşımını olumlu etkilediğini belirtmiştir. Azudin ve arkadaşları (2009: 157) informel iletişimin bilgi paylaşım üzerine etkisini inceledikleri nitel çalışmada, informel iletişimin bilgi paylaşımını olumlu etkilediği sonucuna ulaşmışlardır. Nie, Lin, Ma ve Nakamori (2010), örgüt

içerisindeki informel iletişim ile örtük bilgi paylaşma arasındaki ilişkiyi inceledikleri çalışmada, informel iletişim ve örtük bilgi paylaşımı arasında pozitif bir ilişki olduğunu belirlemişlerdir.

Alan yazın incelendiğinde açık ve örtük bilgi paylaşımının güven, işbirliği, örgüt kültürü, içsel ve dışsal motivasyon, iş deneyimi ile yakından ilişkili olduğu çalışmalara rastlanmıştır (Chen vd., 2011; Wang, Yin, Ma ve Liao, 2021; Salameh ve Zamil, 2020; Fischer, 2021 Imron vd., 2021; Malik, 2021; Santos, Oliveira, ve Curado, 2021). Açık ve örtük bilgi paylaşımla yakından ilişkili olan değişkenlerin formel ve informel iletişimle de ilişki olabileceği söylenebilir. Bu bağlamda örgüt içerisindeki formel ve informel iletişimin olumlu değişim göstermesi amacı ile bu değişkenlere yönelik çalışmalar gerçekleştirilebilir. İlgili alan yazın ve araştırma sonucunda elde edilen bulgular ışığında açık ve örtük bilgi paylaşımı ile formel ve informel iletişimin ilişkili olduğu söylenebilir. Bu bağlamda örgüt içerisinde açık ve örtük bilgi paylaşımının teşvik edilmesi, örgüt içerisindeki formel ve informel iletişimin arttırılmasına olumlu katkı sağlayacağı düşünülmektedir.

"Açık ve örtük bilgi paylaşımı informel iletişim üzerinden dolaylı ve pozitif yönde kurumsal bilgi güvenliğini etkilemektedir." hipotezi reddedilmiştir (H14, H16). Açık ve örtük bilgi paylaşımının kurumsal bilgi güvenliği ile arasında informel iletişimin aracılık etkisinin olmadığı söylenebilir.

Açık ve örtük bilgi paylaşımı formel iletişim üzerinden dolaylı ve pozitif yönde kurumsal bilgi güvenliğini etkilemektedir (H11, H12, H13, H15). Tamjidyamcholo, Bin Baba, Shuib ve Rohani (2014) sanal topluluklarla gerçekleştirdikleri çalışmada bilgi paylaşım davranışı ile bilgi güvenliği riski azaltma beklentisi arasında pozitif ve güçlü bir ilişki olduğu sonucuna ulaşmışlardır. Baran ve Şener (2020b) gerçekleştirdiği çalışmada örgütsel bilgi paylaşım reddi ile bilgi güvenliği kültürü arasında negatif yönlü bir ilişki olduğu belirlenmiştir. Bu sonuca göre örgüt içerisinde bilgi paylaşımı arttıkça bilgi güvenliğinin arttığı bulgulanmıştır (Baran ve Şener, 2020b). Benzer bir çalışmada örgütsel bilgi paylaşımı ve kurumsal bilgi güvenliği arasında pozitif yönlü anlamlı bir ilişki olduğu sonucuna ulaşılmıştır (Baran ve Şener, 2020a). Araştırma sonucunda elde edilen bulgulardan yola çıkarak kurum içerisindeki formel iletişimin arttırılarak açık ve örtük bilgi paylaşımının teşvik edilmesi; böylelikle kurumsal bilgi güvenliğinin sağlanmasına olumlu katkıda bulunacağı düşünülmektedir.

Formel iletişim kurumsal bilgi güvenliğini doğrudan etkilemenin yanı sıra açık ve örtük bilgi paylaşımı ile kurumsal bilgi güvenliği arasında aracılık etmektedir. Bu durum kurumsal bilgi güvenliğinin formel iletişimden güçlü bir şekilde etkilendiği anlamına gelmektedir. Kurum içerisindeki güçlü bir formel iletişimin kurumsal bilgi güvenliğini daha iyi tahmin edeceği düşünülmektedir. Bu nedenle kurumsal bilgi güvenliğini sağlamaya yönelik gerçekleştirilecek çalışmaların formel iletişimi dikkate alarak yapılması gerektiği düşünülmektedir.

Ayrıca bu araştırma problemine yönelik analizlerle kurumsal bilgi güvenliği ile ilgili literatürde yer alan araştırma önerileri, teorik bilgilere yönelik bulgular sunulmuştur. Bu bağlamda kurumsal bilgi güvenliği, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımına yönelik yeni bulgularla alan yazına katkı sağladığı düşünülmektedir.

5.4. Dördüncü Araştırma Problemine İlişkin Sonuç ve Tartışma

Üniversitede görev yapan akademik ve idari personelin kurumsal bilgi güvenliğinin veri madenciliği yöntemleri ile tahmin başarımının incelendiği araştırma problemine ilişkin sonuçlar ve tartışmaya yer verilmiştir. Bu tez çalışmasında kurumsal bilgi güvenliğinin, kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımı bağlamında değerlendirilmesi amacıyla

korelasyon analizi, regresyon analizi ve yapısal eşitlik modellemesi gerçekleştirilmiştir. Bu analizlerin yanı sıra veri madenciliğinin tahmin modelleri ile analizler gerçekleştirilerek sonuçların karşılaştırılması, benzerlik ve farklılıkların ortaya çıkartılması da amaçlanmıştır. Kurumsal bilgi güvenliğinin çıkış değişkeni; saldırı ve tehditler, kişisel verilerin korunması, formel iletişim, informel iletişim, açık bilgi paylaşımı, örtük bilgi paylaşımı giriş değişkeni olarak belirlendiği analiz sonucunda %79'unu tahmin başarımında bulunmuştur. Bu çalışma kapsamında gerçekleştirilen regresyon analizi, YEM sonuçları veri madenciliği sonuçlarıyla benzerdir ve birbirini doğrular niteliktedir. Bu bağlamda veri madenciliği alternatif bir analiz yöntemi olarak kullanılabilir. Araştırma sonucunda elde edilen bulgular ışığında kurumsal bilgi güvenliğinin sağlanmasında, kişisel verilerin korunması ile saldırı ve tehditlere yönelik farkındalığın arttırılmasına yönelik faaliyetler yapılmasının; formel iletişim, informel iletişim, açık ve örtük bilgi paylaşımının teşvik edilmesinin önemli olduğu söylenebilir.

6. ÖNERİLER

Araştırma sonucunda elde edilen bulgular ışığında uygulayıcılara ve araştırmacılara bazı öneriler sunulmuştur.

Uygulayıcılara Yönelik Öneriler

- Bu çalışma ile yöneticilerin kurumsal bilgi güvenliğini sağlamasına katkı sağlayacak bulgular yer almıştır. Yöneticiler kurumsal bilgi güvenliğini sağlamak amacı ile kişisel bilgi güvenliği farkındalığı, örgütsel iletişim ve örgütsel bilgi paylaşımını dikkate alarak tedbirler alabilirler.
- Üniversitede görev yapan akademik ve idari personelin kişisel bilgi güvenliği farkındalığı, kurumsal bilgi güvenliği üzerinde doğrudan ilişkilidir. Kurumlar bilgi güvenliği ihlalleriyle etkin bir şekilde mücadele etmek için kişisel bilgi güvenliği farkındalığının rolünü göz önüne alarak önlemler alabilir.
- Teknoloji her geçen gün daha fazla gelişmektedir. Teknolojide yaşanan gelişmeler ışığında bilgi güvenliğinin sağlanması için yenilikler takip edilerek çalışanlar bu konular hakkında bilgilendirilebilir ve uygulamalar yapılabilir.
- Çalışanların bilgi güvenliği farkındalık düzeyini izlemek ve iyileştirmek için örgüt, teknoloji ve insan açısından stratejiler yapılabilir.
- Üniversiteler, üniversite bilgi ve verileri ile ilgili karşılaşabilecekleri tehlike ve tehditleri öngörmek için sürekli ve periyodik olarak önlemler geliştirmeli; bu tehdit ve önlemleri çalışanları ile paylaşmalıdır. Böylelikle kurumsal bilgi güvenliğinin sağlanması için çalışanların farkındalıkları, bilgi ve becerileri arttırılabilir.
- İlgili alan yazında bilgi güvenliği farkındalığına yönelik eğitimlerin bilgi güvenliği risklerini azaltılmasında etkili olan faktörler arasında yer aldığını bulgulayan çalışmalar bulunmaktadır. Üniversitede görev yapan akademik ve idari personelin kişisel bilgi güvenliği farkındalığını arttıracak eğitimler düzenlenmeli, bu davranışlar teşvik edilmelidir. Düzenlenen eğitimlerle çalışanların bilgi güvenliği farkındalığına yönelik bilgi ve becerileri güncel tutulabilir. Aynı zamanda sızma testleri ve denetlemeler yapılarak çalışanların bilgi güvenliği davranışları kontrol edilebilir.
- Kurumlar bilgi güvenliği zafiyetlerinin kaynaklarını (çalışanlar, teknolojik alt yapı, örgütsel yapı vb.) araştırarak bu konulara yönelik tedbir çalışmaları yapabilir.

- Kurumlar, kişisel bilgi güvenliği farkındalığını etkileyen uyumluluk, kültür gibi faktörlere yönelik çalışmalar yaparak kurumsal bilgi güvenliğinin sağlanmasına katkıda bulunulabilir.
- Kişisel bilgi güvenliği farkındalığı, informel iletişim ve örgütsel bilgi paylaşma düzeyi yaşa, hizmet süresi değişkenine göre anlamlı farklılık göstermesi nedeniyle uygulayıcılar kişisel bilgi güvenliği farkındalığı, informel iletişim ve örgütsel bilgi paylaşmaya yönelik gerçekleştirecekleri çalışmada yaş, hizmet süresi gibi değişkenleri de dikkate alarak önlemler alabilirler. Örneğin farklı yaş ve deneyime sahip çalışanlar için farklı tedbirler alınabilir, grup çalışmaları düzenlenebilir, deneyim paylaşımı için olumlu örgüt kültürü veya iletişim ortamı oluşturulabilir.
- Araştırma sonucunda, kurumsal bilgi güvenliğinin örgüt içerisindeki formel iletişimden pozitif yönde etkilendiği belirlenmiştir. Üniversitede görev yapan akademik ve idari personel arasında olumlu örgüt kültürü, yönetime etkin katılım, paylaşımlı ofisler kullanımı, işyerinde güven ortamının oluşturulması gibi çalışmalarla formel iletişim teşvik edilmeli, böylelikle kurumsal bilgi güvenliğine olumlu katkı sağlanabilir.
- Bilgi paylaşımı ve örgütsel iletişim arasında pozitif yönlü bir ilişki olması nedeniyle üniversitelerde bilgi paylaşımının arttırılmasına yönelik olarak yapıcı bir iletişim ve güven ortamı sağlanabilir.
- Alan yazında yer alan bulgular ve teorik bilgiler örgütsel iletişimin örgütsel bağlılık, örgüt kültürü, liderlik biçimi ile yakından ilişkili olduğunu göstermektedir. Kurum yöneticileri kurumsal bilgi güvenliğinin sağlanmasına katkıda bulunmak amacı ile örgütsel iletişimle yakından ilişkili olan örgütsel bağlılık, örgüt kültürü gibi faktörlerin gelişimine yönelik çalışmalar gerçekleştirebilirler.
- Kurumsal bilgi güvenliğinin sağlanmasında formel iletişimi anlamak, geliştirmek ve değiştirmek için gerekli olan faktörlere odaklanılabilir. Böylelikle zaman ve kaynaklar etkin bir biçimde kullanılabilir. Ayrıca formel iletişim ile açık ve örtük bilgi paylaşımı arasında pozitif yönlü bir ilişki olması nedeniyle formel iletişimin olumlu yönde değişimine yapılacak çalışmalar kurum içerisindeki açık ve örtük bilgi paylaşımını da olumlu etkileyebilir. Bu nedenle formel iletişimin (örgüt kültürü, örgütsel bağlılık, liderlik tarzı) olumlu değişimine yönelik çalışmalar gerçekleştirilebilir.
- Üniversitede görev yapan akademik ve idari personelin örgüt içerisindeki açık ve örtük bilgi paylaşımının arttırılmasına yönelik faaliyetler gerçekleştirilebilir. Üniversiteler araştırma projelerinde, danışmanlık ve akademik çalışmalarda daha fazla ekip çalışması teşvik edilerek bilgi paylaşımı arttırılabilir.
- Araştırma sonucunda bilgi paylaşımının yaş ve mesleki deneyime göre anlamlı farklılık gösterdiği belirlenmiştir. Genç ve yaşlı çalışanlar arasındaki bilgi paylaşımı teşvik edilmesine yönelik grup çalışmaları, işbirliği, deneyim paylaşım toplantıları, iletişimin desteklenmesi gibi çalışmalar gerçekleştirilebilir.
- Örgüt içerisindeki açık ve örtük bilgi paylaşımının teşvik edilmesi kurumsal bilgi güvenliğinin sağlanmasına olumlu katkıda bulunulabilir.
- Örgüt içerisindeki açık ve örtük bilgi paylaşımı ile kurumsal bilgi güvenliği arasındaki ilişkinin belirlenmesinde formel iletişimin aracı değişken olduğu belirlenmiştir. Bu noktadan yola çıkarak örgüt içerisinde formel iletişim arttırılmasına yönelik çalışmalar

yapılarak kurum içerisinde örtük ve açık bilgi paylaşımı ile kurumsal bilgi güvenliğinin olumlu etkilenmesi sağlanabilir.

Araştırmacılara Yönelik Öneriler

- Bu çalışma tek bir üniversitede çalışan akademik ve idari personel ile gerçekleştirilmiştir. Farklı üniversitelerde görev yapan akademik ve idari personel ile de benzer araştırmalar yapılabilir.
- Kamu kurumları kar amacı gütmeyen kuruluşlar olması nedeni ile gelecek çalışmalarda özel sektörde kurumsal bilgi güvenliğini etkileyecek faktörlerin belirlenmesine yönelik benzer araştırmalar gerçekleştirilebilir.
- Kişisel bilgi güvenliği farkındalığını etkileyen uyumluluk, kültür gibi faktörlere yönelik çalışmalar yapılarak kurumsal bilgi güvenliğinin sağlanmasına katkıda bulunulabilir.
- Araştırma sonucunda kişisel bilgi güvenliği farkındalığının kurumsal bilgi güvenliği farkındalığını doğrudan etkiye sahip olması nedeniyle gelecek çalışmalarda kişisel bilgi güvenliği farkındalığı ile ilişkili değişkenlere (vicdanlılık, uyumluluk, kültür gibi) odaklanarak kurumsal bilgi güvenliği üzerindeki etkileri incelenebilir.
- Bu çalışmada kurumsal bilgi güvenliği genel olarak incelenmiştir. Gelecek çalışmalarda kurumsal bilgi güvenliğinin temel unsurları arasında yer alan kullanılabilirlik, erişilebilirlik, gizlilik gibi değişkenlerine odaklanan araştırmalar yapılarak bilgi güvenliğini etkileyen değişkenler detaylı incelenebilir.
- Bu çalışmada örgüt yapısıyla ilişkili olan örgütsel iletişimin kurumsal bilgi güvenliği ile arasındaki ilişki incelenmiştir. Gelecek çalışmalarda örgüt yapısı hakkında bilgi veren farklı değişkenlerin kurumsal bilgi güvenliği ile ilişkisi incelenebilir.
- Kurumsal bilgi güvenliği ile ilgili çalışmalar gerçekleştirilirken formel iletişimin ilişkili olduğu örgüt kültürü, örgütsel bağlılık gibi değişkenler de incelenebilir.
- Bu çalışmada örgütsel iletişim formel ve informel iletişim olarak incelenmiş ve örgütsel iletişim ile ilgili daha fazla bilgi edinilmeye çalışılmıştır. Örgüt içerisindeki iletişim hakkında daha fazla bilgi sağlaması nedeniyle gelecek çalışmalarda örgütsel iletişim, formel ve informel iletişim olarak daha detaylı incelenebilir.
- Bu çalışmada bilgi paylaşımı örtük ve açık bilgi paylaşımı olarak incelenmiş ve bilgi paylaşımı ile ilgili daha fazla bilgi edinilmeye çalışılmıştır. Bilginin doğası gereği açık ve örtük bilgi şeklinde olması, kurum içerisindeki bilgi paylaşımı hakkında daha fazla bilgi vermesi nedeniyle gelecek çalışmalarda bilgi paylaşımı, örtük ve açık bilgi paylaşımı olarak detaylandırılarak incelenebilir.
- Örgüt içerisindeki bilgi paylaşımı ve kurumsal bilgi güvenliği arasındaki ilişkinin belirlenmesinde örgütsel iletişim aracı değişken olarak kullanılmıştır. Bilgi paylaşımını etkileyen veya etkileyebilecek farklı örgütsel ve kişisel unsurlar belirlenerek kurumsal bilgi güvenliği üzerindeki etkisi incelenebilir.
- Gerçekleştirilen tez çalışmasında veri madenciliğinin tahmin modellerinden Yapay Sinir Ağları, Destek Vektör Makineleri, K-En Yakın Komşu ve Rastgele Orman yöntemleri kullanılmıştır. Gelecek çalışmalarda veri madenciliğinin diğer tahmin edici modelleri ve tanımlayıcı modelleri kullanılarak analizler gerçekleştirilebilir.
- Öz bildirime dayalı olan anket çalışmalarında, araştırma katılımcıların yanıtları ile sınırlıdır. Anket çalışması ile birlikte izleme, uygulama, sızıntı testleri gibi çalışmalar yapılabilir. Elde edilen sonuçlar karşılaştırılabilir.

- Bu tez çalışması nicel araştırma yöntemlerinden ilişkisel tarama modeline göre tasarlanmıştır. Kurumsal bilgi güvenliğini etkileyen değişkenlerin belirlenmesi amacıyla nitel veya karma model araştırmaları yapılabilir.

KAYNAKLAR

Abdelwahed, A. S., Mahmoud, A. Y., & Bdair, R. A. (2016). Information security policies and their relationship with the effectiveness of the management information systems of major Palestinian Universities in the Gaza strip. *International Journal of Information Science and Management (IJISM)*, *15*(1), 1-26. https://doi.org/98.1000/1726-8125.2017.15.1.0.1.73.112

Ackoff, R. L. (1989). From data to wisdom. *Journal of applied systems analysis*, *16*(1), 3-9.

Affandie, A. A., Sulistiyono, A., Mayasari, D., Suyono, J., & Elisabeth, D. R. (2020). *The mediating role of organizational commitment in relationship between organizational communication on knowledge sharing*. Proceedings of the 2nd African International Conference on Industrial Engineering and Operations Management Harare, Zimbabwe, December 7-10, 2020.

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: Its antecedents and measures. *Procedia Computer Science, 72, 361–373.* https://doi.org /10.1016/j.procs.2015.12.151

Aghedr, M. M. R. (2021). *Örgütsel iletişim ve bilgi paylaşımının iç müşteri ilişkileri yönetimi üzerine etkisi*. (Doktora tezi). Kastamonu Üniversitesi, Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı, Kastamonu.

Akgül, İ. & Yavuz, U. (2021). Örtülü bilgi paylaşımı ile çalışan yaratıcılığı arasındaki ilişkide algılanan örgütsel desteğin aracı rolü. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 25 (1), 193-213.

Akgün, A. E., Keskin, H., & Günsel, A. (2009). *Bilgi yönetimi ve öğrenen örgütler*. Eflatun Yayınevi.

Akhtar, M. F. (2016). k-nearest neighbor classification I. Hofmann, M., & Klinkenberg, R. (Eds.). *RapidMiner: Data Mining Use Cases and Business Analytics Applications*, 33-41. CRC Press.

Aktan, E. (2017). *Örgüt kültürünün bilgi güvenliği algısı üzerine etkisi: Türkiye'deki devlet üniversitelerinde bir araştırma.* (Doktora tezi). Gazi Üniversitesi, Bilişim Enstitüsü. Ankara.

Aktan, C. C., & Vural, İ. Y. (2016). Bilgi çağında bilginin yönetimi. *Yeni Türkiye 88(1),* Bilim ve Teknoloji Özel Sayısı, 1-15.

Akyol, F. (2013). COBIT (Bilgi ve ilgili teknolojiler için kontrol hedefleri) uygulayan şirketlerdeki bilgi güvenliği politikalarının şirket, personel ve süreçlere etkileri (Yüksek lisans tezi). Beykent Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Alarifi, A., Tootell, H., & Hyland, P. (2012). *A study of information security awareness and practices in Saudi Arabia. 2012 International Conference on Communications and Information Technology (ICCIT).* doi: 10.1109/iccitechnol.2012.6285

Alasulu, N. (2012). *Bilgi güvenliği ve kalite yönetim sistemleri arasındaki ilişkinin incelenmesi ve bir uygulama.* (Yüksek lisans tezi), Fırat Üniversitesi Fen Bilimleri Enstitüsü.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), 432-445. https://doi.org/10.1016/j.cose.2009.12.005.

Alemdaroglu, A. (2020). *Çalışanların bilgi güvenliği farkındalığına ilişkin algıları: bankacılık sektöründe bir araştırma*. (Yüksek lisans tezi), İstinye Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, *3*(3), 176-183.

Alshboul, A. (2010). Information systems security measures and countermeasures: Protecting organizational assets from malicious attacks. *Communications of the IBIMA 2010, 1-9*.

AlKalbani, A., Deng, H., & Kam, B. (2014). A conceptual framework for information security in public organizations for e-government development. 25th Australasian Conference on Information Systems 8 -10 December 2014, Auckland, New Zealand.

AlKalbani, A., Deng, H., & Kam, B. (2019). The Influence of Organizational Enforcement on the Attitudes of Employees towards Information Security Compliance. In *2019 10th International Conference on Information and Communication Systems (ICICS)*, 152-159. IEEE.

Allameh, S. M., Pool, J. K., Jaberi, A., & Soveini, F. M. (2014). Developing a model for examining the effect of tacit and explicit knowledge sharing on organizational performance based on EFQM approach. *Journal of Science & Technology Policy Management*, 5(3), 265-280. https://doi.org/10.1108/jstpm-05-2014-0025.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). *Information security policy compliance: The role of information security awareness.* Proceedings of the Eighteenth Americas Conference on Information Systems, Seattle, Washington, August 9-12, 2012, 1-8.

Altınpulluk, Ö. (2016). *ISO 27001: 2013 Bilgi güvenliği yönetim sistemi kurumsal risk yönetimi.* Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü. İstanbul.

Altındiş, S., & Ağca, V. (2011). Örgütsel Bilgi Paylaşımını Engelleyen Faktörler: Sağlık Sektöründe Bir Görgül Araştırma. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (26), 45-61.

Altun, R. (2014). *Belirli kısıtlara göre bilgi güvenliği ihlallerinin tespiti.* (Yüksek lisans tezi). Beykent Üniversitesi Fen Bilimleri Üniversitesi. İstanbul.

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. (Second Edition) Syngress. USA.

Andrioni, F., & Popp, L. E. (2012). Organizational communication in social care organizations from hunedoara county, Romania. *Procedia-Social and Behavioral Sciences*, *62*, 590-594. https://doi.org/10.1016/j.sbspro.2012.09.099.

Antoniou, G. S. (2015). *Designing an effective information security policy for exceptional situations in an organization: An experimental study*. (Doktora tezi). Nova Southeastern University.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). *Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437–443.* doi: 10.1016/j.chb.2016.12.040

Arhin, K., & Wiredu, G. O. (2018). An organizational communication approach to ınformation security. *The African Journal of Information Systems*, *10*(4), 261-277.

Arslan, N., & Afat, N., (2019). Öğretmenlerin informal iletişim düzeyleri ile örgütsel sinizm arasındaki ilişkinin incelenmesi. *İZÜ Eğitim Dergisi*, *1*(2), 218-249.

Ashenden, D. (2018). *In their own words: employee attitudes towards information security. Information and Computer Security, 26(3), 327–337.* doi: 10.1108/ics-04-2018-0042

Aslan Öztezcan B. (2017). *Bilgi güvenliği farkındalığı üzerine bir araştırma: Marmara Üniversitesi örneği.* (Yüksek lisans tezi). Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Aslan, M. F. (2014). *İşletmelerde bilgi paylaşımı, inovasyon ve firma performansı ilişkisi: Gaziantep ilinde bir araştırma.* (Yüksek lisans tezi). Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü, Gaziantep.

Aslandağ, K. (2010). *Bilgi güvenliği kavramı ve bilgi güvenliği yönetim sistemleri ile şirket performansı ilişkisine dair bir uygulama.* (Yüksek lisans tezi). Gebze Yüksek Teknolojiler Enstitüsü Sosyal Bilimler Enstitüsü, Gebze.

Ataş Akdemir, Ö. (2019). Teachers' Organizational Communication and Their Job Motivation. *Journal of Education and Learning*, *8*(2), 264-270.

Athanassiou, N., & Nigh, D. (2000). Internationalization, tacit knowledge and the top management teams of MNCs. *Journal of international business studies,* 31(3), 471-487. https://doi.org/10.1057/palgrave.jibs.8490917.

Auxier, B., & Anderson, M. (2021). Social media use in 2021. *Pew Research Center*, *1*, 1-4.

Aydoğmuş, E. (2010). *Assessment of information security maturity levels and ISO/IEC 27001: 2005 compliance of organizations in Turkey.* (Yüksek lisans tezi). İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Azudin, N., Ismail, M. N., & Taherali, Z. (2009). Knowledge sharing among workers: a study on their contribution through informal communication in Cyberjaya, Malaysia. *Knowledge Management & E-Learning: An International Journal*, *1*(2), 139-162. https://doi.org/10.34105/j.kmel.2009.01.011.3.

Baker, K. A. (2007). Organizational communication. *Management Benchmark Study*, 1-15.

Baker, R. S. (2014). Educational Data Mining: An Advance for Intelligent Systems in Education. *IEEE Intelligent Systems,* 29(3), 78–82. doi: 10.1109/mis.2014.42

Baker, R. S., & Inventado, P. S. (2014). *Educational Data Mining and Learning Analytics. Learning Analytics, 61–75*. doi: 10.1007/978-1-4614-3305-7_4.

Baran, S. (2019). *Örgütsel bilgi paylaşımının bilgi güvenliği üzerine etkisinin incelenmesi.* (Yüksek lisans tezi). Kırşehir Ahi Evran Üniversitesi Sosyal Bilimler Enstitüsü. Kırşehir.

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

Baran, S., & Şener, E. (2020b). Örgütsel bilgi paylaşım reddi ile bilgi güvenliği kültürü ilişkisinin incelenmesi. *Itobiad: Journal of the Human & Social Science Researches*, *9*(1), 299-325.

Barnard, C. I. (1968). *The functions of the executive*. Harvard University press.

Bartol, K. M., & Srivastava, A. (2002). Encouraging knowledge sharing: The role of organizational reward systems. *Journal of leadership & organizational studies*, *9*(1), 64-76. https://doi.org/10.1177/107179190200900105.

Başdinkçi, N. (2017). *Sağlık kurumlarında bilgi güvenliği risk değerlendirmesi ve kullanıcıların bilgi güvenliği farkındalık düzeyinin ölçülmesi* (Yüksek lisans tezi). Çukurova Üniversitesi Fen Bilimleri Enstitüsü, Adana.

Bellinger, G., Castro, D., & Mills, A. (2004). Data, information, knowledge, and wisdom. https://homepages.dcc.ufmg.br/~amendes/SistemasInformacaoTP/TextosBasicos/Data-Information-Knowledge.pdf (Erişim tarihi: 13.12.2020).

Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. *Information Management & Computer Security*, *13*(3), 189-202. https://doi.org/10.1108/09685220510602013.

Beken, S. (2019). A*n Information security rısk assessment model based on bayesian networks and fuzzy inference system.* (Yüksek lisans tezi). Dokuz Eylül Üniversitesi Fen Bilimleri Enstitüsü. İzmir.

Bhatt, G. D. (2000). Organizing knowledge in the knowledge development cycle. *Journal of knowledge management*, *4*(1), 15-26. https://doi.org/10.1108/13673270010315371.

Bhattacharya, D. (2008). *Leadership styles and information security in small businesses: An empirical investigation*. (Doktora tezi). University of Phoenix.

Bilen, A. (2016). *Bir kurumun bilgi güvenliği farkındalığının incelenmesi.*(Yüksek lisans tezi) Fırat Üniversitesi Fen Bilimleri Enstitüsü. Elazığ.

Bingöl, C. (2010). *ISO 27001 bilgi güvenliği yönetim sistemi otomasyonu.* (Yüksek lisans tezi), Sakarya Üniversitesi Sosyal Bilimleri Enstitüsü, Sakarya.

Blazenaite, A. (2011). Effective organizational communication: In search of a system. *Social Sciences*, *74*(4), 84-101. https://doi.org/10.5755/j01.ss.74.4.1038

Boland, R. J., & Tenkasi, R. V. (1995). Perspective Making and Perspective Taking in Communities of Knowing. *Organization Science, 6(4), 350–372.* doi: 10.1287/orsc.6.4.350

Borca, C., & Baesu, V. (2014). A Possible managerial approach for ınternal organizational communication characterization. *Procedia-Social and Behavioral Sciences,* 124, 496-503.

Boisot, M., & Canals, A. (2004). Data, information and knowledge: have we got it right?. *Journal of Evolutionary Economics*, *14*(1), 43-67.

Boulesteix, A. L., Janitza, S., Kruppa, J., & König, I. R. (2012). Overview of random forest methodology and practical guidance with emphasis on computational biology and bioinformatics. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *2*(6), 493-507.

Bulgurcu, B., Çavuşoğlu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548. https://doi.org/25750690.

Bulut, R. C. (2019). Ortaokulda görev yapan öğretmenlerin iletişim becerileri ile örgütsel sinizm düzeyleri arasındaki ilişki (Yüksek Lisans Tezi). İstanbul Sabahattin Zaim Üniversitesi Sosyal Bilimler Enstitüsü.

Büyüköztürk, Ş. (2012). Sosyal bilimler için veri analizi el kitabı. 14 Baskı. Ankara: Pegem Akademi.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. F., Karadeniz, Ş., & E., Demirel, (2012). Bilimsel araştırma yöntemleri. Pegem Akademi, Ankara.

Cabrera, E. F., & Cabrera, A. (2005). Fostering knowledge sharing through people management practices. *The international journal of human resource management*, *16*(5), 720-735. https://doi.org/10.1080/09585190500083020.

Cabrera, A., Collins, W. C., & Salgado, J. F. (2006). Determinants of individual engagement in knowledge sharing. *The International Journal of Human Resource Management*, *17*(2), 245-264. https://doi.org/10.1080/09585190500404614.

Canary, H. E., & McPhee, R. D. (2010). Introduction: Toward a communicative perspective on organizational knowledge. In H. E. Canary & R. D. McPhee (Eds.), *Communication and organizational knowledge: Contemporary issues for theory and practice* (1–14). Routledge/Taylor & Francis Group.

Canlı, C. (2009). *Saldırı tespit sistemlerinin incelemesi ve bu bağlamda bilgi güvenliği.* (Yüksek lisans tezi). Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Canoğulları, E. (2021). Öğretmenlerin bilgi güvenliği konusundaki farkındalıklarının incelenmesi. *Kalem Eğitim ve İnsan Bilimleri Dergisi, 11(2), 651-679.*

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of ITSecurity management: four ımprovements to current security practices. *Communications of the Association for Information Systems*, *14*(1), 3, 65-75.

Cebula, J. L., & Young, L. R. (2010). *A taxonomy of operational cyber security risks*. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Champoux, J. E. (2010). *Organizational behavior: Integrating individuals, groups, and organizations*. Routledge.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of information privacy and security*, *1*(3), 18-41. https://doi.org/10.1080/15536548.2005.10855772.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106(3)*, 345-361.

Chen, C. A., & Hsieh, C. W. (2015). Knowledge sharing motivation in the public sector: the role of public service motivation. *International Review of Administrative Sciences*, *81*(4), 812-832. https://doi.org/10.1177/0020852314558032.

Chen, G. L., Ling, W. Y., Yang, S. C., Tang, S. M., & Wu, W. C. (2011). Explicit knowledge and tacit knowledge sharing. In *2011 International Conference on Management and Service Science*, 1-4. IEEE. https://doi.org/10.1109/ICMSS.2011.5998951

Cheng, M. Y., Ho, J. S. Y., & Lau, P. M. (2009). Knowledge sharing in academic institutions: A study of Multimedia University Malaysia. *Electronic Journal of Knowledge Management*, *7*(3), 313-324.

Chilton, M. A., & Bloodgood, J. M. (2008). The dimensions of tacit & explicit knowledge: A description and measure. *International Journal of Knowledge Management (IJKM)*, *4*(2), 75-91. https://doi.org/10.1109/HICSS.2007.524.

Chu, A. M., & So, M. K. (2020). Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective . *Sust ainability*, *12*(8),1-25. https://doi.org/10.3390/su12083163.

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics*, 35(6), 1770–1780. doi: 10.1016/j.tele.2018.05.005

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. Second Edition, Lawrence Erlbaum Associates, Publishers .

Cohen, L., Manion, L., & Morrison, K. (2005). *Research methods in education.* (5rd Edition). Taylor & Francis Group.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days?. *Information security technical report*, *14*(4), 186-196. https://doi.org/ 10.1016 /j.istr.2010.04.004.

Contractor, N. S., & Eisenberg, E. M. (1990). Communication networks and new media in organizations. In J. Fulk & C. W. Steinfield (Eds.), *Organizations and communication technology* (143–172). Sage Publications, Inc.

Çanak, M. & Avcı, Ö. Y. (2016). Öğretmenlerin örgütsel özdeşleşme ve örgütsel iletişim düzeylerinin incelenmesi. *Uluslararası Eğitim Bilimleri Dergisi, 3 (7), 91-110.*

Çatuk, Ç. (2018). *Siber riskler karşısında KOBİ'lerin bilgi güvenliği farkındalıklarını ölçen bir ölçek geliştirme: Gaziantep örneklemi.* Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü, Gaziantep.

Çelik, U., Akçetin, E. & Gök, M. (2017). *Rapidminer ile uygulamalı veri madenciliği.* Pusula Yayıncılık. İstanbul.

Çelik Çöp, Ç. (2017*). Kalite yönetim direktörlerinin bilgi güvenliği farkındalığı: İstanbul ili örneği.* Okan Üniversitesi Sağlık Bilimleri Enstitüsü, İstanbul.

Çek, E. (2017). *Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği için insan faktörünün önemi.* (Yüksek lisans tezi), İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul

Çetinkaya, M. (2008). *Bilgi güvenliği yönetim sistemi alt yapısının değerlendirilmesi için bir test aracı geliştirilmesi*. (Yüksek lisans tezi). İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Çokluk, Ö., Şekercioğlu, G., & Büyüköztürk, Ş. (2018). Sosyal bilimler için çok değişkenli istatistik: SPSS ve LISREL uygulamaları. (2. Baskı) PegemAkademi, Ankara.

Çuhadar, C., Özgür, H., Akgün, F., & Gündüz, Ş. (2014). Öğretmen adaylarının iletişim becerileri ve iletişimci biçimleri. *Ahi Evran Üniversitesi Kırşehir Eğitim Fakültesi Dergisi*, *15*(1), 295-311.

Daniel, E. C., & Eze, O. L. (2016). The role of formal and informal communication in determining employee affective and continuance commitment in oil and gas companies. *International Journal of Advanced Academic Research-Social & Management Sciences*, *2*(9), 33-44.

Devasia, T., Vinushree, T. P., & Hegde, V. (2016). Prediction of students performance using Educational Data Mining. In *2016 International Conference on Data Mining and Advanced Computing (SAPIENCE)* (pp. 91-95). IEEE. https://doi.org/10.1109/sapıence.2016.7684167.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 1-23. https://doi.org/10.1016/j.cose.2020.101713

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business Press.

Demirok, E. (2016). Kurumsal bilgi güvenliği yönetim sistemi uygulaması: Vakıf üniversitesi örneği. Yayınlanmamış (Yüksek lisans tezi). İstanbul: Okan Üniversitesi Fen Bilimleri Enstitüsü İstanbul.

Demirtaş, H. (2013). Bilgi güvenliği yönetiminin gerekleri ve başarı dayanakları: Bir uygulama örneği (Yüksek lisans tezi), Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya.

DeSanctis, G., & Monge, P. (1999) Introduction to the Special Issue: Communication Processes for Virtual Organizations. *Organization Science*, 10(6): 693-703. https://doi.org/10.1287/orsc.10.6.693.

Dhillon, G., & Backhouse, J. (2000). *Technical opinion: Information system security management in the new millennium. Communications of the ACM, 43(7), 125–128.* doi: 10.1145/341852.341877.

Diesch, R., Pfaff, M., ve Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers ve Security*, *92*, 101747. https://doi.org/10.1016/j.cose.2020.101747.

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2008). Information security: The moving target. *Computers & security*, *28*(3-4), 189-198. https://doi.org/10.1016/j.cose.2008.11.007.

Efeoğlu, İ. E. & Çetin, S. (2012). Örgütsel iletişimin değerlendirilmesi: belediyelere dair uygulamalı bir çalışma. *Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi, 21(3), 185-204.*

Efron, B., & Tibshirani, R. J. (1994). *An introduction to the bootstrap.* CRC press.

Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. *Computer Fraud & Security*, *2005*(11), 10-16. https://doi.org/10.1016/S1361-3723(05)70275-X.

Eminağaoğlu, M. (2011). *Özdevimli öğrenme yaklaşımı ile bilgi güvenliği risklerinin nitel değerlendirilmesine yönelik bir model.* (Doktora tezi). Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report,* 14(4), 223–229. https://doi.org/10.1016/j.istr.2010.05.002

Ender Akcan, G. (2019). *Özel sağlık sigorta şirketleri çalışanlarının elektronik sağlık kayıtlarının gizliliği ve güvenliği hakkında görüşlerinin değerlendirilmesi*. (Yüksek lisans tezi), Marmara Üniversitesi, Sağlık Bilimler Enstitüsü, Sağlık Yönetimi Ana Bilim Dalı, İstanbul.

Erden, H. (2016). *KOBİ'lerde bilgi paylaşımı: Konya ili Ereğli ilçesinde gıda işletmelerinde bir inceleme.* (Yüksek lisans tezi), Çağ Üniversitesi Sosyal Bilimler Enstitüsü, Mersin.

Ergen, G. (2007). *Developıng an information security management framework: case studies on registration office and computer center of a state university.* (Yüksek lisans tezi). Boğaziçi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Ernest Chang, S., & Lin, C. (2007). *Exploring organizational culture for information security management. Industrial Management & Data Systems,* 107(3), 438–458. https://doi.org/10.1108 /0263557 0710734316

Ernita, H., Ruldeviyani, Y., Maftuhah, D. N., & Mulyadi, R. (2022). Strategy to Improve Employee Security Awareness at Information Technology Directorate Bank XYZ. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *6*(4), 577-584. https://doi.org/10.29207/resti.v6i4.4170

Ertürk, R., & Aydın, B. (2018). Yeniçağa ve Dörtdivan İlçelerindeki Okullarda Örgütsel İletişim ve İşe Angaje Olma Davranışı: Öğretmen Görüşlerine Dayalı İlişkisel Bir Analiz. *Adnan Menderes Üniversitesi Eğitim Fakültesi Eğitim Bilimleri Dergisi*, *9*(2), 86-99.

Eslamkhah, M., & Seno, S. A. H. (2019). Identifying and ranking knowledge management tools and techniques affecting organizational information security improvement. *Knowledge Management Research & Practice, 1-30*. https://doi.org/10.1080/14778238.2019.1599495.

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

Filik, T., & Ünalan, D.(2021). The Evaluatıon of the effect of the ınformatıon securıty awareness level in medical secretaries on the security and privacy implementations of electronic health records. *Hacettepe Sağlık İdaresi Dergisi*, *24*(1), 183-202.

Fish, R. S., Kraut, R. E., Root, R. W., & Rice, R. E. (1992). Evaluating video as a technology for informal communication. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, 37-48. doi: 10.1145/142750.142755

Fischer, C. (2021). Incentives Can't Buy Me Knowledge: The missing effects of appreciation and aligned performance appraisals on knowledge sharing of public employees. *Review of Public Personnel Administration*,1-22. https://doi.org/10.1177/0734371X20986839

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90-110. https://doi.org/10.1016/j.cose.2014.03.004.

François, M. T. (2016). *A quantitative study on the relationship of information security policy awareness, enforcement, and maintenance to information security program effectiveness*. (Doktora Tezi). Capella University.

Fulford, H., & Doherty, N.F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation, *Information Management & Computer Security*, 11 (3), 106-114. https://doi.org/10.1108/09685220310480381.

Furnell, S., & Rajendran, A. (2012). Understanding the influences on information security behaviour. *Computer Fraud & Security*, *2012*(3), 12-15. https://doi.org/10.1016/S1361-3723(12)70053-2.

Fullwood, R., Rowley, J., & McLean, J. (2019). Exploring the factors that influence knowledge sharing between academics. *Journal of Further and Higher Education*, *43*(8), 1051-1063. https://doi.org/10.1080/0309877X.2018.1448928

Fullwood, R., & Rowley, J. (2017). *An investigation of factors affecting knowledge sharing amongst UK academics. Journal of Knowledge Management, 00–00.* doi: 10.1108/jkm-07-2016-0274

Galvez, S. M., & Guzman, I. R. (2009). Identifying factors that influence corporate information security behavior. *AMCIS 2009 Proceedings*, *San Francisco, California August 6th-9th* 1-11.

Ganbat, O. (2013). *Bilgi güvenliği yönetim sistemi ISO/IEC 27001 ve bilgi güvenliği risk yönetimi ISO/IEC 27005 standartlarının uygulanması*.(Yüksek lisans tezi), Ege Üniversitesi Fen Bilimleri Enstitüsü, İzmir.

Gemci, C. (2010). *Uzman sistem temelli bilgi güvenliği yönetim sistemi yaklaşımı.* (Doktora tezi). Gazi Üniversitesi Bilişim Enstitüsü, Ankara.

Gencer, K. (2015). *ISO 27001 kapsamında kurumsal bilgi güvenliğine dinamik bir yaklaşım.* (Yüksek lisans tezi). Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyonkarahisar.

Genç, C. (2019). *Kişisel verilerin korunması kapsamında bilgi güvenliği farkındalığı analizi ve e-devlet yapısının incelenmesi.* (Yüksek lisans tezi). İstanbul Okan Üniversitesi Fen Bilimleri Enstitüsü. İstanbul.

Gerçeker, B. (2012). *Sağlık kuruluşlarında örgüt iklimi ve bilgi güvenliğinin ilişkisi.* (Yüksek lisans tezi). Dokuz Eylül Üniversitesi Sağlık Bilimleri Enstitüsü. İzmir.

Giri, V. N., & Kumar, B. P. (2010). Assessing the impact of organizational communication on job satisfaction and job performance. *Psychological Studies*, *55*(2), 137-143.

Gizir, S., & Simsek, H. (2005). Communication in an academic context. *Higher Education,* 50(2), 197–221. doi: 10.1007/s10734-004-6349-x

Gochhayat, J., Giri, V. N., & Suar, D. (2017). Influence of organizational culture on organizational effectiveness: The mediating role of organizational communication. *Global Business Review*, *18*(3), 691-702. https://doi.org/10.1177/0972150917692185.

Goh, S. K., & Sandhu, M. S. (2013). Knowledge Sharing Among Malaysian Academics: Influence of Affective Commitment and Trust. *Electronic Journal of Knowledge Management*, *11*(1), 38-48.

Grama, J. L. (2020). *Legal and Privacy Issues in Information Security*. Jones & Bartlett Learning.

Gregory, P. H. (2003). *Enterprise information security: information security for non-technical decision makers*. Financial Times Prentice Hall.

Guffey, M. E., & Loewy, D. (2021). *Business communication: Process & product*. Cengage Learning.

Gumus, M. (2007). The effect of communication on knowledge sharing in organizations. *Journal of Knowledge Management Practice*, 8(2), 15-26.

Gurteen, D. (1999). Creating a knowledge sharing culture. *Knowledge Management Magazine*, *2*(5), 1-4.

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

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

Günbayi, I. (2007). The organizational communication process in schools. *Kuram ve Uygulamada Egitim Bilimleri,* 7(2), 787-798.

Güngör, G., & Celep, C. (2016). Ortaöğretim öğretmenlerinin örgüt içi bilgi paylaşımı, örgütsel öğrenme ve entelektüel sermaye düzeyleri arasındaki ilişki. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, *12*(3), 932-947. https://doi.org/10.17860/mersinefd.282391

Gürbüz, S. (2021). Sosyal Bilimlerde Aracı, Düzenleyici ve Durumsal Etki Analizleri. (2. Baskı). Seçkin Yayıncılık Ankara.

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

Gyllensten, K., & Torner, M. (2021). The role of organizational and social factors for information security in a nuclear power industry. *Organizational Cybersecurity Journal: Practice, Process and People*. https://doi.org/10.1108/OCJ-04-2021-0012.

Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I., & Jones, K. (2019). Exploring the role of work identity and work locus of control in information security awareness. *Computers & Security*, *81*, 41-48. https://doi.org/10.1016/j.cose.2018.10.006.

Haeussinger, F. & Kranz, J. (2017). *Antecedents of employees' information security awareness - review, synthesis, and directions for future research.* In Proceedings Of The 25th European Conference On Information Systems (Ecıs), Guimarães, Portugal, June 5-10, 2017.

Han, J., & Kamber, M. (2011). *Data mining: concepts and techniques*. Second Edition. Elsevier.

Han, D., Dai, Y., Han, T., & Dai, X. (2015). Explore awareness of information security: insights from cognitive neuromechanism. *Computational intelligence and neuroscience*, *2015,* 1-8. https://doi.org/10.1155/2015/762403.

Haroon, H., & Malik, H. D. (2018). The impact of organizational communication on organizational performance. *Journal of Research in Social Sciences*, *6*(2), 140-151.

Harrington, D. (2009). *Confirmatory factor analysis.* Oxford university press.

Harris, C., Hedges, L., & Valentine, J. (2019). *Handbook of research synthesis and meta-analysis*. (3rd Edition). Russell Sage Foundation, New York.

Hau, Y. S., Kim, B., Lee, H., & Kim, Y. G. (2013). The effects of individual motivations and social capital on employees' tacit and explicit knowledge sharing intentions. *International Journal of Information Management*, *33*(2), 356-366. https://doi.org/10.1016/j.ijinfomgt.2012.10.009.

Hedges, L. V. (2019). Statistical Considerations. Handbook of research synthesis and meta-analysis. C. Harris, L. Hedges, & J. Valentine (Ed.). *Handbook of research synthesis and meta-analysis* (3rd Edition) içinde (37-48), Russell Sage Foundation, New York.

Henkoğlu, T. (2015). *Hassas bilgi varlıklarının ve kişisel verilerin hukuksal düzenlemeler ile korunması ve bu kapsamda üniversiteler için bilgi güvenliği politikasının geliştirilmesi*, (Doktora tezi). Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Hofmann, M., & Klinkenberg, R. (Eds.). (2016). *RapidMiner: Data mining use cases and business analytics applications*. CRC Press.

Howells, J. (1996). Tacit knowledge. *Technology Analysis & Strategic Management,* 8(2), 91–106. doi: 10.1080/09537329608524237

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say?. *Computers & security*, *21*(5), 402-409. https://doi.org/10.1016/S0167-4048(02)00504-7.

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1-55. https://doi.org/10.1080/10705519909540118

Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, *31*(4), 6-48. https://doi.org/10.1080/07421222.2014.1001255.

Hua, J., & Bapna, S. (2013). Who can we trust?: the economic impact of insider threats. *Journal of Global Information Technology Management*, *16*(4), 47-67. https://doi.org/10.1080 /1097198X .2013.10845648.

Hwang, S. (2020). Sharing tacit knowledge in small-medium regional construction companies in the US: the current status and the impact of organizational ecology. *International Journal of Construction Management*, 1-10. https://doi.org/10.1080/15623599.2020.1742628

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security Awareness: The First Step in Information Security Compliance Behavior. *Journal of Computer Information Systems*, 1–12. https://doi.org/10.1080/08874417.2019.1650676

ISO/IEC, 2005 ISO/IECISO/IEC 27002, (2005): code of practice for information security management. https://www.iso.org/standard/50297.html (ErişimTarihi: 01.03. 2022)

Ipe, M. (2003). Knowledge sharing in organizations: A conceptual framework. *Human resource development review*, *2*(4), 337-359. https://doi.org/10.1177/1534484303257985.

Imron, M. A., Munawaroh, U. I., Farida, R. D. M., Paramarta, V., Sunarsi, D., Akbar, I. R., ... & Masriah, I. (2021). Effect of organizational culture on innovation capability employees in the knowledge sharing perspective: Evidence from digital industries. *Annals of the Romanian Society for Cell Biology*, 4189-4203.

İnce, M., & Gül, H. (2011). The role of the organizational communication on employees' perception of justice: a sample of public ınstitution from Turkey. *European Journal of Social Sciences*, *21*(1), 106-124.

Jahani, S., Ramayah, T., & Effendi, A. A. (2011). Is reward system and leadership important in knowledge sharing among academics. *American Journal of Economics and Business Administration*, *3*(1), 87-94.

Jarrahi, M. H. (2017). Social Media, Social Capital, and Knowledge Sharing in Enterprise. IT Professional, 20(4), 37–45. doi: 10.1109/mitp.2017.265105759

Jiang, Z., & Hu, X. (2015). *Knowledge Sharing and Life Satisfaction: The Roles of Colleague Relationships and Gender. Social Indicators Research, 126(1), 379–394.* doi: 10.1007/s11205-015-0886-9

Jones, C. M. (2009). *Utilizing the technology acceptance model to assess employee adoption of information systems security measures*. (Doktora tezi). Nova Southeastern University.

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy*, *5*(3), 16-24. https://doi.org/10.1109/MSP.2007.59.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496. https://doi.org/10.1016/j.procs.2014.05.452.

Kahraman, S. (2006). *Yönetimde bilgi güvenlik sisteminin yapısı, işleyişi ve Aselsan AŞ'de uygulaması.* (Yüksek lisans tezi). Anadolu Üniversitesi Sosyal Bilimler Enstitüsü. Eskişehir.

Kamath, R. S., & Kamat, R. K. (2016). *Educational data mining with R and rattle*. River Publishers.

Kampanakis, P. (2014). Security automation and threat information-sharing options. *IEEE Security & Privacy*, *12*(5), 42-51.

Kandemirli, B. M. (2012). *Bilgi teknolojileri güvenliği ve sigorta şirketinde ISO/IEC 27001 standartları çerçevesinde bilgi güvenlik yönetim sistemi uygulaması.* (Yüksek lisans tezi). Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Kantardzic, M. (2011). *Data mining: concepts, models, methods, and algorithms*. John Wiley & Sons.

Kapanoğlu, G. (2016). *Öğretmenlerin Bilgi Güvenliği Farkındalığının İncelenmesi.* (Yüksek lisans tezi). Gazi Üniversitesi Eğitim Bilimleri Enstitüsü. Ankara.

Karabatak, S., & Karabatak, M. (2019). Information Security Awareness of School Administrators. *2019 7th International Symposium on Digital Forensics and Security (ISDFS).* doi: 10.1109/isdfs. 2019.8757525

Karasar, N. (2011). *Bilimsel araştırma yöntemi,* 22. Baskı. Nobel Yayın Dağıtım. Ankara.

Karimi, O. (2018). *İnsan faktörünü içeren bilgi güvenliği çerçevesi için kavramsal bir model oluşturmak*. (Doktora tezi). İstanbul Üniversitesi Fen Bilimleri Enstitüsü. İstanbul.

Kartal, C. (2020). Destek Vektör Makineleri ile Borsa Endekslerinin Tahmini. *Itobiad: Journal of The Human & Social Science Researches*, *9*(2), 1394-1418.

Katırcı, C. (2021). *Kamu sektöründe X ve Y kuşaklarının örgütsel iletişim değerleri üzerine bir araştırma.* (Yüksek lisans tezi). İzmir Kâtip Çelebi Üniversitesi Sosyal Bilimler Enstitüsü. İzmir.

Keser, H., & Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği (Bgfö) Geliştirme. *Kastamonu Eğitim Dergisi*, *23*(3), 1167-1184.

Keyton, J. (2010). *Communication and organizational culture: A key to understanding work experiences*. Sage Publications.

Keyton, J. (2017). Communication in Organizations. *Annual Review of Organizational Psychology and Organizational Behavior, 4(1), 501–526.* doi: 10.1146/annurev-orgpsych-032516-113341.

Khadraoui, D., & Francine, H. (2007). Advances in enterprise information technology security ınformation. *Science Reference (IGI Global), New York*.

Khan, A., Ibrahim, M., & Hussain, A. (2021). An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. *International Journal of Information Management Data Insights, 1(2), 100015.* doi: 10.1016/j.jjimei.2021.100015

Kılcıgil, E., Bilir, P., Özdinç, Ö., Eroğlu, K., & Eroğlu, B. (2009). İki farklı üniversitenin beden eğitimi ve spor yüksekokulu öğrencilerinin iletişim becerilerinin değerlendirilmesi. *Spormetre Beden Eğitimi ve Spor Bilimleri Dergisi*, *7*(1), 19-28. https://doi.org/10.1501/Sporm_0000000145.

Kızılelma. T. T. (2014). *An analysis of the relationships among information security management systems, patient safety, and quality*. (Doktora tezi). Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir.

Kim, H. L., & Han, J. (2019). Do employees in a "good" company comply better with information security policy? A corporate social responsibility perspective. *Information Technology & People*. 32 (4), 858-875. https://doi.org/10.1108/ITP-09-2017-0298.

King, W. R. & He, J. (2011). Knowledge sharing. D. G. Schwartz & D. Te'eni (Ed.), *In Encyclopedia of Knowledge Management,* Second Edition (914-923). IGI Global.

Kline, R. B. (2015). *Principles and practice of structural equation modeling*. Guilford publications.

Kline, P. (1994). An easy guide to factor analysis.Routledge.London and Newyork

Kocamustafaoğulları, M. (2013). *Bilgi güvenliği farkındalığı ve uygulama seviyesi değerlendirmek için bilgi güvenliği prototip uygulaması*. (Yüksek lisans tezi), Çankaya Üniversitesi Bilgi Teknolojileri Ana Bilim Dalı. Ankara.

Koch, T., & Denner, N. (2022). Informal communication in organizations: work time wasted at the water-cooler or crucial exchange among co-workers?. *Corporate Communications: An International Journal*. https://doi.org/10.1108/CCIJ-08-2021-0087

Koç, N. (2017). *İşletmelerde bilgi güvenliği için web tabanlı bir uygulamanın geliştirilmesi*. (Yüksek lisans tezi), Mersin Üniversitesi Sosyal Bilimler Enstitüsü. Mersin.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, *28*(7), 509-520.

Kraut, R. E., Fish, R. S., Root, R. W., & Chalfonte, B. L. (1990). Informal communication in organizations: Form, function, and technology. In *Human reactions to technology: Claremont symposium on applied social psychology*. 145-199.

Kurt, H. Ö. (2019). *Kurumlarda bilgi güvenliği yönetimi: hastane bilgi sistemleri üzerine bir araştırma.* (Yüksek lisans tezi). Necmettin Erbakan Üniversitesi Sağlık Bilimleri Enstitüsü. Konya.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. In *2013 46th Hawaii International Conference on System Sciences*, 2978-2987. IEEE.

Lee, V. C. (2015). *Examining the Relationship between Autonomy, Competence, and Relatedness and Security Policy Compliant Behavior*. (Doktora tezi). Northcentral University.

Lee, H. S., & Kim, J. K. (2010). Relationship among Communication Competence, Communication Types, and Organizational Commitment in Hospital Nurses. Journal of Korean Academy of Nursing Administration, 16(4), 488. https://doi.org/10.11111/jkana.2010.16.4.488

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

Liebowitz, J., & Megbolugbe, I. (2003). A set of frameworks to aid the project manager in conceptualizing and implementing knowledge management initiatives. *international Journal of project management*, *21*(3), 189-198. https://doi.org/10.1016/S0263-7863(02)00093-5.

Liew, A. (2007). Understanding data, information, knowledge and their inter-relationships. *Journal of knowledge management practice*, *8*(2), 1-16.

Liu, Y., Tse, W. K., Kwok, P. Y., & Chiu, Y. H. (2022). Impact of Social Media Behavior on Privacy Information Security Based on Analytic Hierarchy Process. *Information*, *13*(6), 280. https://doi.org/10.3390/info13060280

Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management*, 54, 1-14. https://doi.org/10.1016/j.ijinfomgt.2020.102152

Lunenburg, F. C. (2010). Formal communication channels: Upward, downward, horizontal, and external. *Focus on Colleges, Universities, and Schools*, *4*(1), 1-7.

MacKinnon, D. P., Fairchild, A. J., & Fritz, M. S. (2007). *Mediation Analysis. Annual Review of Psychology, 58(1), 593–614.* doi: 10.1146/annurev.psych.58.1104.

Mahabi, V. (2010). *Information security awareness: system administrators and end-users perspectives at florida state university.* (Doktora tezi). Florida State University.

Malik, S. (2021). The nexus between emotional intelligence and types of knowledge sharing: does work experience matter?. *Journal of Workplace Learning*. 33(8), 619-634. https://doi.org/10.1108/JWL-10-2020-0170.

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32-44. https://doi.org/10.1016/j .chb. 2018.01.028

Marques, J. F. (2010). Enhancing the quality of organizational communication. *Journal of Communication Management, 14 (1),* 47-58. doi: 10.1108/13632541011017807.

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

Matej, M., & Miroslav, P. (2016). Medical Data Mining. Hofmann, M., & Klinkenberg, R. (Eds.). *RapidMiner: Data mining use cases and business analytics applications*, 289-317.

Martins, A., & Eloff, J. (2002). Information security culture. *In Security In The Information Society*, 203-214. Springer, Boston, MA.

Matzler, K., Renzl, B., Müller, J., Herting, S., & Mooradian, T. A. (2008). Personality traits and knowledge sharing. *Journal of economic psychology*, *29*(3), 301-313. https://doi.org/10.1016/j.joep.2007.06.004.

May, L., & Lane, T. (2006). A Model for improving e-Security in Australian Universities. *Journal of Theoretical and Applied Electronic Commerce Research*, *1*(2), 90-96. https://doi.org/10. 3390/jtaer1020016

McMillan, J. H., & Schumacher, S. (2014). *Research in Education: Evidence-Based Inquiry*. (7rd Edition). MyEducationLab Series. Pearson.

McCormac A., Zwaans T., Parsons K., Calic D., Butavicius M. & Pattinson M. (2017). Individual differences and Information Security Awareness, *Computers in Human Behavior*, https://doi.org/10.1016/j.chb.2016.11.065

McGill, T. and Thompson, N. (2018) *Gender differences in information security perceptions and behaviour.* In: Australasian Conference on Information Systems 2018, 3 - 5 December 2018, UTS, Sydney

Melenli, İ. (2011). *Örgütsel faktörlerin bilgi paylaşma davranışına etkisi: Bir uygulama*. (Yüksek lisans tezi). Beykent Üniversitesi Sosyal Bilimler Enstitüsü. İstanbul.

Men, L. R. (2014). Why Leadership Matters to Internal Communication: Linking Transformational Leadership, Symmetrical Communication, and Employee Outcomes. *Journal of Public Relations Research*, 26(3), 256–279. https://doi.org/10.1080/1062726x.2014.908719

Mete, H. (2010). *ISO/IEC 27001 Bilgi güvenliği yönetim sistemi'nin bilgi işlem merkezlerinde uygulanması.* Sakarya Üniversitesi Sosyal Bilimler Enstitüsü. Sakarya.

Meydan, C. H., ve Şeşen, H. (2015). Yapısal Eşitlik Modeli AMOS Uygulamaları. (2. Baskı) Detay Yayıncılık, Ankara.

Miller, K. I. (2008). *Organizational Communication.* Donsbach, W. (ed.) *The International Encyclopedia of Communication* içinde (3415-3428). Wiley Publishing. doi: 10.1002/9781405186407.wbieco018.

Miller, K. (2011). Organizational communication: Approaches and processes 8th ed. *WADSWORTH CENGANGE Learning, Boston*.

Miller, D. L., & Karakowsky, L. (2005). *Gender Influences as an Impediment to Knowledge Sharing: When Men and Women Fail to Seek Peer Feedback. The Journal of Psychology, 139(2), 101–118.* doi: 10.3200/jrlp.139.2.101-118

Mitchell, H. (2005). Knowledge sharing: The value of story telling. *International Journal of Organisational Behaviour*, *9*(5), 632-641.

Mitrofan, N., & Bulborea, A. (2013). The role of organizational communication in structuring interpersonal relationships. *Procedia-Social and Behavioral Sciences*, *76*, 511-515. https://doi.org/10.1016/j .sbspro.2013.04.155

Muharremoğlu, G. (2013). *Kurumsal bilgi güvenliğinde zafiyet, saldırı ve savunma öğelerinin incelenmesi*. (Yüksek lisans tezi), İstanbul Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Murphy, E. M. (2017). *Internal strategies for assessing organizational communication channel effectiveness.* (Doktora tezi). Walden University.

Mutahar, Y., Farea, M. M., Abdulrab, M., Al-Mamary, Y. H., Alfalah, A. A., Alshallaqi, M., & Grada, M. (2022). The contribution of trust to academic knowledge sharing among academics in the Malaysian research institutions. *Cogent Business & Management*, *9*(1), 1-16. https://doi.org/10.1080/23 311975.2022.2038762.

Narain Singh, A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*, *27*(5), 644-667. https://doi.org/10.1108/ JEIM-07-2013-0052.

Neher, W. W. (1997). *Organizational communication: Challenges of change, diversity, and continuity*. Boston, MA: Allyn and Bacon.

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

Nie, K., Lin, S., Ma, T., & Nakamori, Y. (2010). Connecting informal networks to management of tacit knowledge. *Journal of Systems Science and Systems Engineering*, *19*(2), 237-253.

Nişancı, Z. N., & Bakkal, E. (2020). Hizmet inovasyonu, bilgi paylaşımı ve işgören tatmini arasındaki ilişki: bir çağrı merkezi örneği. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, *19*(39), 898-924. https://doi.org/10.46928/iticusbe.760495

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford university press.

Oliveira, M. J. S. P., & Pinheiro, P. (2021). Factors and barriers to tacit knowledge sharing in non-profit organizations–A case study of volunteer firefighters in Portugal. *Journal of the Knowledge Economy*, *12*(3), 1294-1313.

Oksa, R., Kaakinen, M., Savela, N., Ellonen, N., & Oksanen, A. (2020). *Professional social media usage: Work engagement perspective. New Media & Society, 23(8), 2303–2326.* doi: 10.1177/1461444820921938

Okul, T., Şimşek, G., Hafçı, B., & Barış, Z. (2018). Bilgi güvenliği farkındalığı: Kuşadası'ndaki beş yıldızlı oteller örneği. *Uluslararası Türk Dünyası Turizm Araştırmaları Dergisi*, *3*(2), 189-201.

Ölçer, N., & Koçer, S. (2015). Örgütsel iletişim: Kocaeli Üniversitesi akademik personeli üzerine bir inceleme. *Global Media Journal TR Edition,* 6(11), 339-383.

Öneren, M., Çiftçi, G. E., & Harman, A. (2016). Bilgi paylaşımının yenilikçi davranışa ve örgütsel güvene etkisi üzerine bir araştırma. *Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi*, (58), 127-157.

Özcan, B., (2009). *Kurumsal bilgi güvenliği & COBIT.* (Yüksek lisans tezi). Haliç Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Özkan, Y. (2020). *Veri madenciliği yöntemleri.*(3. Baskı) Papatya Yayıncılık Eğitim. İstanbul.

Özdemir, A. (2019). *Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı.* (Yüksek lisans tezi). Gazi Üniversitesi, Bilişim Enstitüsü, Ankara.

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

Özdemir-Güngör, D., Kıdak, L. B., & Ercan, Y. (2018). Formal communication channels in a state hospital: a qualitative study. *İİOAB Journal,* 9(6), 48-55.

Özhan, M. (2019). *The effects of information security domains on reputation of financial institutions.* (Yüksek lisans tezi), Marmara Universitesi Sosyal Bilimler Enstitüsü. İstanbul.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, *42*, 165-176. https://doi.org/10.1016/j.cose.2013.12.003.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117-129. https://doi.org/10.1177/1555343415575152.

Peltier, T. R. (2013). *Information security fundamentals*. CRC press.

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), 489-510. https://doi.org/10.1515/jhsem-2014-0035.

Polat, V., Lynn, G., Akgün, A., & Emre, O. (2018). Formal and informal communication in new product development teams: the mediation effect of team trust. *International Journal of Innovation*, *6*(2), 97-111. http://dx.doi.org/10.5585/iji.v6i2.245.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & security*, *23*(8), 638-646. https://doi.org/10.1016/j.cose.2004.10.006

Postmes, T., Tanis, M., & de Wit, B. (2001). *Communication and Commitment in Organizations: A Social Identity Approach. Group Processes & Intergroup Relations, 4(3), 227–246.* https://doi.org/10.1177/1368430201004003004

Pratiyush, G. & Manu, S. (2016). Classifying educational data using support vector machines: A supervised data mining technique. *Indian Journal of Science and Technology*, *9*, 34. DOI: 10.17485/ijst/2016/v9i34/100206

Puspitaningrum, E. A., Devani, F. T., Putri, V. Q., Hidayanto, A. N., & Hapsari, I. C. (2018). Measurement of employee information security awareness: case study at a government institution. In *2018 Third*

International Conference on Informatics and Computing (ICIC), pp. 1-6. IEEE. doi: 10.1109/iac.2018.8780571

Rader, E., Wash, R., & Brooks, B. (2012). *Stories as informal lessons about security. Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12.* https://doi.org/10.1145/2335356.2335364

Rader, E., & Wash, R. (2015). *Identifying patterns in informal sources of security information. Journal of Cybersecurity, tyv008.* https://doi.org/10.1093/cybsec/tyv008

Rahman, M. S., Mannan, M., Hossain, M. A., Zaman, M. H., & Hassan, H. (2018). Tacit knowledge-sharing behavior among the academic staff: Trust, self-efficacy, motivation and Big Five personality traits embedded model. *International Journal of Educational Management*. 32 (5), 761-782. https://doi.org/10.1108/IJEM-08-2017-0193.

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

Rajhans, K. (2012). Effective organizational communication: A key to employee motivation and performance. *Interscience Management Review*, *2*(2), 81-85.

Ramachandran, S. (2007). *An investigation of information security subcultures in organizations: A case study*. (Doktora tezi). The University of Texas at San Antonio.

Ramayah, T., Yeap, J. A., & Ignatius, J. (2014). Assessing knowledge sharing among academics: A validation of the knowledge sharing behavior scale (KSBS). *Evaluation review*, *38*(2), 160-187. https://doi.org/10.1177/0193841X14539685.

Razmerita, L., Kirchner, K., & Nielsen, P. (2016). What factors influence knowledge sharing in organizations? A social dilemma perspective of social media communication. *Journal of Knowledge Management*, 20(6), 1225–1246. https://doi.org/10.1108/jkm-03-2016-0112

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security,* 27(7-8), 241-253. doi: 10.1016/j.cose.2008.07.008.

Robbins, S. P., & Judge, T. A. (2013). *Organizational behavior.* New Jersey: Pearson Education.

Roberts, J. (2000). From know-how to show-how? Questioning the role of information and communication technologies in knowledge transfer. *Technology Analysis & Strategic Management*, *12*(4), 429-443. https://doi.org/10.1080/713698499.

Rocha Flores, W., & Ekstedt, M. (2016). *Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers & Security, 59, 26–44.* https://doi.org/10.1016/j.cose.2016.01.004

Romero, C., & Ventura, S. (2010). Educational data mining: a review of the state of the art. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *40*(6), 601-618.

Romero, C., & Ventura, S. (2013). Data mining in education. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *3*(1), 12-27.

Rooney, D., Hearn, G., & Ninan, A. (Eds.). (2005). *Handbook on the knowledge economy*. Edward Elgar Publishing.

Ross, S. C. (2021). *Organizational Behavior Today*. Routledge. Taylor & Francis.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442-451. https://doi.org/10.1016/j.chb.2015.12.037

Safa, N.S., Von Solms, R., & Furnell, S. (2016). *Information security policy compliance model in organizations. Computers & Security, 56, 70–82.* doi: 10.1016/j.cose.2015.10.006

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, *2016*(2), 15-18. https://doi.org/10.1016/S1361-3723(16)30017-3

Salameh, A., & Zamil, Z. (2020). The effects of reward systems and organizational structure on tacit knowledge sharing. *Management Science Letters*, *10*(10), 2229-2236. https://doi.org/10.5267/j.msl.2020.3.013.

Santos, R. F., Oliveira, M., & Curado, C. (2021). The effects of the relational dimension of social capital on tacit and explicit knowledge sharing: a mixed-methods approach. *VINE Journal of Information and Knowledge Management Systems*. On press. https://doi.org/10.1108/VJIKMS-05-2020-0094.

Sarıkoz, B. G. (2015). An Information security framework for web services in enterprise networks. (Yüksek lisans tezi). Orta Doğu Teknik Üniversitesi Bilişim Sistemleri Enstitüsü, Ankara.

Sari, P. K. (2012). A concept of information security management for higher education. In *International Conference on Technology and Operation Management, 3rd. Bandung*, 469-477.

Sari, P. K., & Prasetio, A. (2017). Knowledge sharing and electronic word of mouth to promote information security awareness in social network site. *2017 International Workshop on Big Data and Information Security (IWBIS).* https://doi.org/10.1109/iwbis.2017.8275111

Sauerwein, C., Pekaric, I., Felderer, M., & Breu, R. (2019). An analysis and classification of public information security data sources used in research and practice. *Computers & Security*, *82*, 140-155. https://doi.org/10.1016/j.cose.2018.12.011.

Sharratt, M., & Usoro, A. (2003). Understanding knowledge-sharing in online communities of practice. *Electronic Journal on knowledge management*, *1*(2), 187-196.

Sheerin, C., Hughes, C., & Garavan, T. (2020). Gendered practices and tacit knowledge sharing in organizations: a structuration perspective. *Human Resource Development International,* 1–27. https://doi.org/10.1080/13678868.2020.1769402

Shochley-Zalabak, P. (2015). Fundamentals of organizational communication. 9. Baskı. Pearson Education.

Smith, E. A. (2001). The role of tacit and explicit knowledge in the workplace. *Journal of knowledge Management,* 5 (4), 311-321. https://doi.org/10.1108/13673270110411733.

Singh, V., & Margam, M. (2018). Information security measures of libraries of Central Universities of Delhi: A study. *DESIDOC Journal of Library & Information Technology*, *38*(2), 102-109. https://doi.org/10.14429/djlit.38.2.11879.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2), 64-71. https://doi.org/10.1109/MC.2010.35.

Sivakumar, S., Venkataraman, S., & Selvaraj, R. (2016). Predictive modeling of student dropout indicators in educational data mining using improved decision tree. *Indian Journal of Science and Technology*, *9*(4), 1-5. https://doi.org/ 10.17485/ijst/2016/v9i4/87032.

Small, C. T. (2005). *An enterprise knowledge-sharing model: A complex adaptive systems perspective on improvement in knowledge sharing*. (Yüksek lisans tezi). George Mason University.

Soliman, W., & Mohammadnazar, H. (2022). New insights into the justifiability of organizational information security policy noncompliance: A Case Study. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. University of Hawai'i at Manoa. 6812-6821 https://doi.org/10.24251/HICSS.2022.823

Stamp, M. (2011). *Information security: principles and practice*. John Wiley & Sons.

Stanton, J. M., Stam, K. R., Guzman, I., & Caledra, C. (2003). *Examining the linkage between organizational commitment and information security*. In SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme-System Security and Assurance (Cat. No. 03CH37483), 3, 2501-2506. IEEE. doi: 10.1109/icsmc.2003.1244259

Sümer, N. (2000). Yapısal eşitlik modelleri: temel kavramlar ve örnek uygulamalar. *Türk Psikoloji Yazilari*, 3 (6), 49-74.

Şen, S. (2020). *Mplus ile yapısal eşitlik modellemesi uygulamaları.* Nobel Akademik Yayıncılık.

Şahinaslan, E. (2010). *Standartlara dayalı bilgi güvenliği risk analiz ve ölçümleme metodolojisinin bankacılık sektörüne özgü modellenmesi ve uygulama yazılımının geliştirilmesi.* (Doktora tezi). Trakya Üniversitesi Fen Bilimleri Enstitüsi, Edirne.

Tabachnick, B. G. & Fidell, L. S., (2007). *Using multivariate statistics*. 5. Bask. Boston, MA: Pearson.

Tamjidyamcholo, A., Bin Baba, M. S., Shuib, N. L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security,* 43, 19–34. https://doi.org/10.1016/j.cose.2014.02.010

Taner, E. (2018). *Güvenlik güçlerinin bilgi güvenliği farkındalığına yönelik bir betimleme*. (Yüksek Lisans Tezi), Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon.

Tang, M., Li, M. G., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, *17*(2), 179-186.

Taylor, W. A., & Wright, G. H. (2004). Organizational readiness for successful knowledge sharing: Challenges for public sector managers. *Information Resources Management Journal (IRMJ)*, *17*(2), 22-37.

Tekin, H. (2004). *Eğitimde ölçme ve değerlendirme.* 17. Baskı, Yargı Yayınları, Ankara.

Tekin, P. (2015). *Kurum içi iletişimin kurum kültürüne etkisi: bir kamu kurumu uygulaması.* İstanbul Gelişim Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Thomson, K. L., Von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer fraud & security*, *2006*(10), 7-11. https://doi.org/10.1016/S1361-3723(06)70430-4

Todisco, L., Tomo, A., Canonico, P., Mangia, G., & Sarnacchiaro, P. (2021). Exploring social media usage in the public sector: Public employees' perceptions of ICT's usefulness in delivering value added. Socio-Economic Planning Sciences, 73, 100858. doi: 10.1016/j.seps.2020.100858

Tok, H. (2010). Kamu kurumları için bilgi güvenliği yönetişim modeli. (Yüksek lisans tezi). Gebze Yüksek Teknoloji Üniversitesi Mühendislik ve Fen Bilimleri Enstitüsü, Gebze.

Topsakaloğlu, S. (2015). *Türk Kamu Yönetiminde Kamu Çalışanları Arasındaki Örgütsel İletişimin Örgütsel Bağlılık Üzerine Etkisi: Mutki İlçesi Örneği.* Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta.

Tu, C. Z., Yuan, Y., Archer, N., & Connelly, C. E. (2018). Strategic value alignment for information security management: a critical success factor analysis. *Information & Computer Security*, *26*(2), 150-170. https://doi.org/10.1108/ICS-06-2017-0042

Tuna, Y. (2008). *Örgütsel iletişim sürecinde yöneticilerin duygusal zeka yeterlilikleri.* (Doktora tezi). Anadolu Üniversitesi Sosyal Bilimler Enstitüsü. Eskişehir.

Turaç, İ. S. (2022). Hemşirelerin Kanıta Dayalı Hemşireliğe Yönelik Tutumları Ve Bilgi Güvenliğinin Hasta Güvenliği Kültürü Üzerine Etkisi. Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü. Ankara.

Tuygun, M. (2019). *ISO27001 Bilgi güvenliği yönetim sistemi standardının kamu kurumlarına uygulanabilirliğinin araştırılması: Ankara ili örneği.* (Yüksek lisans tezi). Gazi Üniversitesi Bilişim Enstitüsü, Ankara.

Uludağ, O., Aktaş, İ., & Özdoğaç Özgit, H. (2019). Eğitim çalışanlarının örgütsel adalet algılarının ve örgüt kültürünün bilgi paylaşımı üzerindeki etkileri: Örgüt kültürünün aracı rolü. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi*, 34(1), 160-181. doi: 10.16986/HUJE.2018037423.

Ulusoy, B. (2015). Bilgi paylaşımı perspektifinde öz yeterliliğin çalışan yaratıcılığına etkisi. (Doktora tezi). İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Uslu, B., & Welch, A. (2016). The influence of universities' organizational features on professorial intellectual leadership. *Studies in Higher Education,* 43(3), 571–585. doi: 10.1080/03075079 .2016.1185774.

Ünver, M. (2019) . *Türkiye'de insan kaynakları yönetiminde bilgi güvenliği uygulamaları.* (Yüksek lisans tezi). Atılım Üniversitesi Sosyal Bilimler Enstitüsü. Ankara.

Van Den Hooff, B., & De Ridder, J. A. (2004). Knowledge sharing in context: the influence of organizational commitment, communication climate and CMC use on knowledge sharing. *Journal of knowledge management*. https://doi.org/10.1108/13673270410567675.

Vander Elst, T., Baillien, E., De Cuyper, N., & De Witte, H. (2010). *The role of organizational communication and participation in reducing job insecurity and its negative association with work-related well-being. Economic and Industrial Democracy, 31(2), 249–264.* doi: 10.1177/0143831x09358372

Vardal, N. (2009). *Yükseköğretimde bilgi güvenliği: Bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması.* (Doktora Tezi). Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Von Solms, B. (2001). Corporate governance and information security. *Computers & Security*, *20*(3), 215-218.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376. https://doi.org/10.1016/j.cose.2004.05.002

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & security*, *23*(3), 191-198. https://doi.org/10.1016/j.cose.2004.01.012.

Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri.* (Yüksek lisans tezi). Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara

Yang, H. L., & Wu, T. C. (2008). Knowledge sharing in an organization. *Technological Forecasting and Social Change*, *75*(8), 1128-1156. https://doi.org/10.1016/j.techfore.2007.11.008.

Yang, S. C., & Farn, C. K. (2009). Social capital, behavioural control, and tacit knowledge sharing—A multi-informant design. *International Journal of Information Management*, *29*(3), 210-218. https://doi.org/10.1016/j.ijinfomgt.2008.09.002

Yao, J., Crupi, A., Di Minin, A., & Zhang, X. (2020). Knowledge sharing and technological innovation capabilities of Chinese software SMEs. *Journal of Knowledge Management*, 24 (3), 607-634. https://doi.org/10.1108/JKM-08-2019-0445.

Yazıcıoğlu, N. (2019). *Kurum içi etkin iletişim ortamı ile örgütsel sinizm arasındaki ilişki* (Yüksek lisans tezi). İstanbul Sabahattin Zaim Üniversitesi, Sosyal Bilimler Enstitüsü, Eğitim Bilimleri Anabilim Dalı, İstanbul.

Yerby, J., & Floyd, K. (2018). Faculty and staff information security awareness and behaviors. *In Journal of The Colloquium for Information Systems Security* Education, 6(1), 1-23.

Yeşil, S. & Mavi, Y. (2021). Örgütsel güvenin bilgi paylaşımına etkisi: bir alan araştırması. *Van Yüzüncü Yıl Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi. 6(11),* 79-100.

Yıldırım, O. (2014). The impact of organizational communication on organizational citizenship behavior: research findings. *Procedia-Social and Behavioral Sciences*, *150*, 1095-1100. https://doi.org/ 10.1016/j.sbspro.2014.09.124.

Yıldız, B. (2007). *Bilgi güvenliği ve e-devlet kapsamında kamu kurumlarında bilgi güvenliği yönetimi standartlarının uygulanması.* (Yüksek lisans tezi). Gebze Yüksek Teknolojiler Üniversitesi Sosyal Bilimler Enstitüsü, Gebze.

Yılmaz, M. (2009). Enformasyon ve bilgi kavramları bağlamında enformasyon yönetimi ve bilgi yönetimi. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, *49*(1).

Yılmaz, V., & Dalbudak, Z. İ. (2018). Aracı değişken etkisinin incelenmesi: yüksek hızlı tren işletmeciliği üzerine bir uygulama. *Uluslararası Yönetim İktisat ve İşletme Dergisi*, *14*(2), 517-534.

Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education*, *6*(2), 26-45. https://doi.org/10.19126/suje.29650

Zawawi, A. A., Zakaria, Z., Kamarunzaman, N. Z., Noordin, N., Sawal, M. Z. H. M., Junos, N. M., & Najid, N. S. A. N. (2011). The study of barrier factors in knowledge sharing: A case study in public university. *Management Science and Engineering*, *5*(1), 59-70. http://dx.doi.org/10.3968/ j.mse.1913035X20110501.007

Zhao, D., & Rosson, M. B. (2009). How and why people Twitter: the role that micro-blogging plays in informal communication at work *Proceedinfs of the ACM 2009 International Conference on Supporting Group Work - GROUP '09.* 243-252. doi: 10.1145/1531674.1531710

Ziegler, A., & König, I. R. (2014). Mining data with random forests: current options for real-world applications. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *4*(1), 55-63.

Waddell, S. A. (2013). *A Study of the effect of ınformation security policies on ınformation security breaches in higher education institutions*. (Doktora tezi). Nova Southeastern University.

Wall, J.D. and Palvia, P. (2022). *Understanding employees' information security identities: an interpretive narrative approach.* Information Technology & People. 35(1), 435-458. https://doi.org/10.1108/ITP-04-2020-0197.

Wang, N., Yin, J., Ma, Z., & Liao, M. (2021). The influence mechanism of rewards on knowledge sharing behaviors in virtual communities. *Journal of Knowledge Management*. On press. https://doi.org/10.1108/JKM-07-2020-0530.

Wang, X., & Xu, J. (2021). *Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry. Tourism Management, 84, 104282*. https://doi.org/ 10.1016/j.tourman.2021.104282

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Wijetunge, P. (2012). Organizational storytelling as a method of tacit-knowledge transfer: Case study from a Sri Lankan university. *The International Information & Library Review,* 44(4), 212-223. https://doi.org/10.1016/j.iilr.2012.09.001

Wiley, A., McCormac, A. & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security, 88,1-8.* https://doi.org/ 10.1016/j.cose.2019.101640.

Williams, P. A. (2008). In a 'trusting'environment, everyone is responsible for information security. *Information Security Technical Report*, *13*(4), 207-215. https://doi.org/ 10.1016/j .istr.2008.10.009

Wilson, D. O. (1992). Diagonal communication links within organizations. *The Journal of Business Communication (1973),* 29(2), 129-143.

Xu, J., Wang, X., & Yan, L. (2021). The moderating effect of abusive supervision on information security policy compliance: Evidence from the hospitality industry. *Computers & Security*, *111*, 102455. https://doi.org/10.1016/j.cose.2021.102455.

EKLER

Ek- 1: Veri Toplama Aracı Uygulama İzin Belgeleri

Evrak Tarih ve Sayısı: 28/01/2020-374677

T.C.

FIRAT ÜNİVERSİTESİ REKTÖRLÜĞÜ

Sosyal Bilimler Enstitüsü

Sayı :17206398/730.08.03/
Konu :Anket Uygulama İzni (Ebru POLAT)

Sayın: Doç. Dr. Ahmet TEKİN

Rektörlük Makamının 27.01.2020 tarih ve 374355 sayılı yazısı ekte gönderilmiştir.
Bilgilerinizi rica ederim.

e-imzalıdır.
Prof. Dr. Ömer Osman UMAR
Enstitü Müdürü

EK :
Rektörlük Makamının 27.01.2020 tarih ve 374355 sayılı yazısı (1 sayfa)
DAĞITIM
Gereği:
Teknoloji ve Bilgi Yönetimi Anabilim Dalına
Bilgi:
Sayın: Doç. Dr. Ahmet TEKİN

T.C.

FIRAT ÜNİVERSİTESİ REKTÖRLÜĞÜ

Genel Sekreterlik

Sayı :11611387/730.08.03/
Konu :Anket İzni (Ebru POLAT)

SOSYAL BİLİMLER ENSTİTÜSÜNE

İlgi :23.01.2020 tarihli ve 17206398/730.08.03/373974 sayılı yazınız.

Enstitünüz Teknoloji ve Bilgi Yönetimi Anabilim Dalı Başkanlığı doktora öğrencisi Ebru POLAT'ın, "Kurumsal Bilgi Güvenliğinin Örgütsel İletişim, Örgütsel Bilgi Paylaşımı ve Kişisel Bilgi Güvenliği Farkındalığı Açısından Değerlendirilmesi" konulu tez çalışması kapsamında geliştirdiği anketi, Üniversitemiz Akademik ve İdari personellerine uygulayabilmesine ilişkin izin talebi Rektörlüğümüz tarafından uygun bulunmuştur.

Bilgileriniz ile gereğini rica ederim.

e-imzalıdır.
Prof. Dr. Sadettin TANYILDIZI
Rektör Yardımcısı

EK :
Yazı (13 Sayfa)

T.C.
DİCLE ÜNİVERSİTESİ REKTÖRLÜĞÜ
Öğrenci İşleri Daire Başkanlığı

Sayı : E-68508712-044-232472 14/02/2022
Konu : Anket İzni

FIRAT ÜNİVERSİTESİ REKTÖRLÜĞÜNE

İlgi : 02/12/2021 tarihli ve 116112 sayılı yazı.

İlgi'de kayıtlı yazınız ile Üniversiteniz Sosyal Bilimler Enstitüsü Teknoloji ve Bilgi Yönetimi Anabilim Dalı doktora programı öğrencisi Ebru POLAT'ın danışmanı Prof. Dr. Ahmet TEKİN yönetiminde yürüteceği, "Kurumsal Bilgi Güvenliğinin Örgütsel İletişim, Örgütsel Bilgi Paylaşımı ve Kişisel Bilgi Güvenliği Farkındalığı Açısından Değerlendirilmesi" başlıklı tez konusu ile ilgili hazırlamış olduğu anketi Üniversitemiz Akademik ve İdari Personellerine uygulama talebi Rektörlüğümüzce uygun görülmüştür.

Bilgilerinize arz ederim.

Prof. Dr. Ahmet TANYILDIZ
Rektör a.
Rektör Yardımcısı

Ek: 8 Sayfa

T.C.
MUNZUR ÜNİVERSİTESİ REKTÖRLÜĞÜ
Personel Daire Başkanlığı

Sayı : E-99161742-044-43717 14.02.2022
Konu : Anket Uygulama İzni

FIRAT ÜNİVERSİTESİ REKTÖRLÜĞÜNE
Fırat Üniversitesi Rektörlüğü Elazığ

İlgi : 02.12.2021 tarihli ve 116112 sayılı yazınız

İlgi yazınız ile belirtilen Üniversiteniz Sosyal Bilimler Enstitüsü Teknoloji ve Bilgi Yönetimi Anabilim Dalı doktora öğrencisi Ebru POLAT'ın danışmanı Prof. Dr. Ahmet TEKİN yönetiminde yürüteceği "Kurumsal Bilgi Güvenliğinin Örgütsel İletişim, Örgütsel Bilgi Paylaşımı ve Kişisel Bilgi Güvenliği Farkındalığı Açısından Değerlendirilmesi" başlıklı tez çalışması için talep edilen anket uygulama izni uygun görülmüştür.

Bilgilerinize arz ederim.

Prof. Dr. Ubeyde İPEK
Rektör

Ek- 2: Etik Kurul Raporu

Evrak Tarih ve Sayısı: 13/12/2019-365105

T.C.

FIRAT ÜNİVERSİTESİ REKTÖRLÜĞÜ

Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu

Sayı :97132852/302.14.01/
Konu :Etik Kurul Değerlendirmesi

TEKNOLOJİ VE BİLGİ YÖNETİMİ ANABİLİM DALINA

Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Öğr.Üyesi Doç.Dr.Ahmet TEKİN'in danışmanı olduğu doktora öğrencisi Ebru POLAT'a ait **"Kurumsal Bilgi Güvenliğinin Örgütsel İletişim, Örgütsel Bilgi Paylaşımı ve Kişisel Bilgi Güvenliği Farkındahğı Açısından Değerlendirilmesi"** konulu çalışma ile ilgili Etik Kurul Kararı ekte sunulmuştur.

Gereğini ve bilgilerinizi rica ederim.

e-imzalıdır.
Prof. Dr. Mehmet Nuri GÖMLEKSİZ
Kurul Başkanı

ETİK KURUL KARARI

TOPLANTI TARİHİ	TOPLANTI SAYISI	KARAR NO	ÇALIŞMACILARIN ADI SOYADI
12.12.2019	40	1	Sorumlu Araştırmacı : Doç.Dr.Ahmet TEKİN Yardımcı Araştırmacı: Ebru POLAT

KARAR

"Kurumsal Bilgi Güvenliğinin Örgütsel İletişim, Örgütsel Bilgi Paylaşımı ve Kişisel Bilgi Güvenliği Farkındalığı Açısından Değerlendirilmesi " konulu çalışma etik kurulumuzda görüşülmüş olup; çalışmanın etik kurallara uygun olduğuna oybirliğiyle karar verilmiştir.

Prof. Dr. Mehmet Nuri GÖMLEKSİZ (Başkan)			
Prof. Dr. Sebahattin DEVECİOĞLU (Üye)	Bulunamadı	Doç. Dr. Rıfat BİLGİN (Üye)	İmza
Doç. Dr. Süleyman İLHAN (Üye)	İmza	Doç.Dr. Haki PEŞMAN (Üye)	İmza
Doç. Dr. İrfan EMRE (Üye)	İmza	Doç.Dr. Yunus Emre KARAKAYA (Üye)	İmza
Doç. Dr. Taner YILDIRIM (Üye)	Bulunamadı	Dr. Öğr. Üyesi Serkan BİÇER (Üye)	İmza
Doç.Dr. Erkan Turan DEMİREL (Üye)	İmza	Dr.Öğr. Üyesi Ayşe Ülkü KAN (Üye)	İmza

ETİK KURUL KARARI

TOPLANTI TARİHİ	TOPLANTI SAYISI	KARAR NO	ÇALIŞMACILARIN ADI SOYADI
04.11.2021	22	5	Sorumlu Araştırmacı : Prof. Dr. Ahmet TEKİN Yardımcı Araştırmacı: Ebru POLAT

KARAR(Düzeltme)

"Kurumsal Bilgi Güvenliğinin Örgütsel İletişim, Örgütsel Bilgi Paylaşımı ve Kişisel Bilgi Güvenliği Farkındalığı Açısından Değerlendirilmesi" konulu çalışma etik kurulumuzda görüşülmüş olup; çalışmanın etik kurallara uygun olduğuna oybirliğiyle karar verilmiştir.

Prof. Dr. Mehmet Nuri GÖMLEKSİZ (Başkan)			
Prof. Dr. Sebahattin DEVECİOĞLU (Üye)	İmza	Doç. Dr. Rıfat BİLGİN (Üye)	İmza
Prof. Dr. Süleyman İLHAN (Üye)	İmza	Doç.Dr. Haki PEŞMAN (Üye)	İmza
Prof. Dr. Kenan PEKER (Üye)	İmza	Doç.Dr. Yunus Emre KARAKAYA (Üye)	İmza
Prof. Dr. İrfan EMRE (Üye)	İmza	Doç.Dr. Ayşe Ülkü KAN (Üye)	İmza
Doç. Dr. Taner YILDIRIM (Üye)	İmza	Dr.Öğr. Üyesi Serkan BİÇER (Üye)	İmza
Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurul Sekreteri: Pınar ARSLAN			İmza

Ek- 3: Veri Toplama Aracı

	Örgütsel İletişim Envanter (Tuna, 2008)	**Asla**	**Nadiren**	**Bazen**	**Sık sık**	**Sürekli olarak**
1	Çalışanlar arasında yüz yüze iletişim imkânları fazladır.					
2	Herhangi bir probleminiz olduğunda fark edilir ve yardım edilir					
3	Kişilerin kendilerini ilgilendiren konularda fikri alınır.					
4	Yapılması gereken isler ilgili kişilere yazılı olarak iletilir.					
5	Tüm çalışanlar kurumla ilgili gelişmelerden hemen haberdar edilir.					
6	Doğum günü parti gibi resmi olmayan toplantılarda çalıştığım kuruma ilişkin edindiğim bilgiler, resmi kanallardan (yazılı iletileri, kurum mailleri resmi yazışmalar gibi) elde ettiğim bilgilerden daha fazladır.					
7	Problemlerin ve görüşlerin yöneticilere iletilmesinde sorun yaşanmaktadır.					
8	Herkesin yaptığı isle ilgili yetki ve sorumlulukları yazılı olarak belirlenmiştir.					
9	İletişim eksikliğinden kaynaklanan çatışmalar yaşanmaktadır.					
10	Bilgilendirme amaçlı iletişim araçları (gazete, yazılı genelgeler, duyurular, raporlar, ilan tahtaları, anons ve radyo sistemi) sürekli kullanılmaktadır					
11	Çalışanlar ve yöneticilerin mesai dışında da görüşme imkânı bulunmaktadır.					
12	Yapılacak is ile ilgili istenenler doğrudan o isi yapacak kişiye değil üst makamına iletilir.					
13	Çalışanlara olan kızgınlık ifadesi doğrudan sözel olarak ifade edilir.					
14	Çalışanlar arasında iyi bir bilgi alışverişi bulunmaktadır					
15	Değişik statü ve kademeye sahip bireylerin oluşturduğu çalışma grupları bulunmaktadır.					
16	Çalışanların doğum günleri evlilik yıldönümleri gibi özel günleri hatırlanır.					
17	Yöneticiler çalışanların performansları ile ilgili yeterli bilgiye sahiptir					
18	Ast üst ilişkilerinde resmiyet vardır.					
19	Yeni ise başlayanlar is ortamına kısa sürede alışırlar.					
20	Bürokratik engeller isleri yavaşlatır.					

Değerli Katılımcı,

Sizi "Kurumsal Bilgi Güvenliği" ile ilgili araştırmaya davet ediyoruz. Araştırmada sizden yaklaşık 15-20 dakika ayırmanız istenmektedir. Bu çalışmaya katılmak tamamen gönüllülük esasına dayanmaktadır. Çalışmanın amacına ulaşması için sizden beklenen, bütün soruları eksiksiz, kimsenin baskısı veya telkini altında olmadan, size en uygun gelen cevapları içtenlikle verecek şekilde cevaplamanızdır. Bu formu okuyup onaylamanız, araştırmaya katılmayı kabul ettiğiniz anlamına gelecektir. Ancak, çalışmaya katılmama veya katıldıktan sonra herhangi bir anda çalışmayı bırakma hakkına da sahipsiniz. Bu çalışmadan elde edilecek bilgiler tamamen araştırma amacı ile kullanılacak olup kişisel bilgileriniz gizli tutulacaktır; ancak verileriniz yayın amacı ile kullanılabilir. Anketteki sonuçlar bilimsel araştırma kapsamında kullanılacağı için vereceğiniz cevaplar samimi ve doğru olması araştırma açısından önemlidir. Bu konuda araştırmanın bir parçası olarak ilgi ve yardımlarınızdan dolayı teşekkür ederiz

Prof. Dr. Ahmet TEKİN

Ebru POLAT

1. Cinsiyetiniz: ( ) Erkek ( ) Kadın
2. Medeni Haliniz: ( ) Evli ( ) Bekâr ( ) Diğer
3. Yaşınız: (Lütfen Yıl Olarak Yazınız) ……..
4. İdari personel için Göreviniz (mutemet, sayman, sekreter, vb.):
   ……
5. Akademik personel için varsa idari göreviniz (dekan, müdür, bölüm başkanı vb.):
   ……
6. Hizmet süreniz: (Lütfen Yıl Olarak Yazınız) ……..
7. Kurumda çalışma süreniz: (Lütfen Yıl Olarak Yazınız) ……..
8. Görev yaptığınız akademik veya idari birim?
   ……
9. Eğitim düzeyiniz?
   - ☐ Lise
   - ☐ Ön lisans
   - ☐ Lisans
   - ☐ Yüksek lisans
   - ☐ Doktora
   - ☐ Diğer (yazınız) ……
10. Bilgisayarı / İnterneti kullanma düzeyiniz?
    - ☐ Düşük
    - ☐ Orta
    - ☐ Yüksek
11. Günlük bilgisayar/İnternet kullanma süreniz?
    - ☐ 0-30 dk
    - ☐ 30 dk- 1 saat
    - ☐ 1-3 saat
    - ☐ 3 saatten fazla
12. Bilgisayarı/İnterneti kaç yıldır kullanıyorsunuz?
    - ☐ 1 yıldan az
    - ☐ 1-3 yıl
    - ☐ 3-5 yıl
    - ☐ 5 yıldan fazla
13. İnterneti kullanma amacınız nedir? (Birden fazla seçeneği tercih edebilirsiniz.)
    - ☐ Konuşma/Mesajlaşma
    - ☐ Oyun oynama
    - ☐ Müzik dinleme
    - ☐ Film/video izleme
    - ☐ Gazete okuma/haber izleme/bilgi edinme
    - ☐ Alışveriş
    - ☐ Sosyal Ağ

☐ Diğer (yazınız) ……..

14. Sosyal Ağ sitelerini kullanım düzeyiniz?
    ☐ Düşük
    ☐ Orta
    ☐ Yüksek
15. İnternette/sosyal ağ sitelerinde ne tür kişisel bilgilerinizi paylaşırsınız? (Birden fazla seçeneği tercih edebilirsiniz.)
    ☐ E-posta adresi
    ☐ Telefon numarası
    ☐ Doğum tarihi
    ☐ Kişisel fotoğraf
    ☐ Kişisel video
    ☐ Diğer (yazınız) ……..
16. İnternette/ sosyal ağ sitelerinde gizlilik/güvenlik ayarlarını hangi sıklıkla kontrol edersiniz?
    ☐ Haftada bir
    ☐ Ayda birkaç defa
    ☐ Ayda bir
    ☐ Yılda birkaç defa
    ☐ Yılda bir
    ☐ Kontrol etmiyorum
17. İnternette gezinirken/ sosyal ağ sitelerinde kişisel bilgilerinizi doğru olarak veriyor musunuz?
    ☐ Evet
    ☐ Hayır
18. İnternet ortamlarının güvenli olduğunu düşünüyor musunuz?
    ☐ Evet
    ☐ Kısmen
    ☐ Hayır
19. İnternet ortamlarında paylaştığınız bilgilerin başkaları tarafından alınıp kullanılabileceğini düşünüyor musunuz?
    ☐ Evet
    ☐ Kısmen
    ☐ Hayır

	Bilgi Güvenliği Ölçeği (Gerçeker, 2012)	**Tamamen Katılmıyorum**	**Katılmıyorum**	**Kararsızım**	**Katılıyorum**	**Tamamen Katılıyorum**
1	Kurumumuzda bilgi güvenliği hedefleri belirlenmiştir.					
2	Kurumsal bilgi güvenliği yönetim sistemi oluşturulmuştur.					
3	Kişisel bilgi güvenliğindeki tehditler ve güvenlik açıklıkları nettir.					
4	Korunacak kişisel bilgiler belirlenmiştir.					
5	Kurumsal bilgi güvenliği kurumsal izlenmektedir.					
6	Kurumuzda bilgi güvenliği uygulamasında yönetim kararlıdır.					
7	Bilgi güvenliği komitesi bulunmaktadır.					
8	Sistematik risk yönetimi uygulaması bulunmaktadır.					
9	Yönetim, kaynakları etkin bir şekilde kullanır.					
10	Benzer kurumlarla bilgi güvenliği kıyaslaması yapılmaktadır.					
11	Bilgi güvenliği iç denetimi yapılmaktadır.					
12	Bilgi güvenliği yönetim sistemi, ilerlemeyi sağlar.					
13	Kişisel bilgilerin korunması gerekli değildir.					
14	Bilgi güvenliği politikası bulunmaktadır.					
15	Bilgi güvenliği sorumluları belirlidir.					
16	Kişisel verilerini korumak için kurallar bulunmaktadır.					
17	Tüm kişisel verileri gizli tutulmalıdır.					
18	Kendi bilgilerimin arkadaşlarım tarafından görülmesini isterim.					
19	Kurumdan ayrılan personelin kullanıcı erişim yetkileri hemen iptal edilir.					
20	Kurumumuzda fiziksel ve çevresel güvenlik sağlanmaktadır.					
21	Kişisel bilgiler şifreli bir formatta tutulmaktadır.					
22	Acil durumlarda erişim kontrol kuralları belirlidir.					
23	Bilgi sistemleri edinmenin kuralları bulunmaktadır.					
24	Bilgi güvenliği güvenlik olayları etkili bir şekilde sonuçlanır.					
25	Kurumumuzda bilgi güvenliği gereklilik olarak kabul edilmiştir.					
26	Bilgi güvenliği yönetim sistemi sağlıklı uygulanmaktadır.					

	Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği (Keser ve Güldüren, 2015)	**Hiç Katılmıyorum**	**Katılmıyorum**	**Kararsızım**	**Katılıyorum**	**Tamamen Katılıyorum**
1	Bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim.					
2	Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum.					
3	Aldatmaca (hoax) nedir biliyorum.					
4	Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.					
5	Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.					
6	Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum.					
7	Kimlik hırsızlığı (identity theft) nedir biliyorum.					
8	Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.					
9	Sahte virüs koruma yazılımının ne olduğunu biliyorum.					
10	Hizmet aksatrma (Denial of Service - DoS) saldırısı nedir biliyorum.					
11	Kimlik avı (phishing) saldırısı nedir biliyorum.					
12	Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.					
13	Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.					
14	Siber zorbalık (cyberbullying) nedir biliyorum.					
15	Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.					
16	Siber zorbalığa karşı çocuklarımı nasıl koruyacağımı biliyorum.					
17	Bilgi güvenliğinin ne anlama geldiğini biliyorum.					
18	Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.					
19	Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.					
20	Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum.					
21	Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım.					
22	Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.					
23	Dijital imza (digital signature) nedir biliyorum.					
24	Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.					
25	E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.					
26	İstenmeyen elektronik posta (spam) nedir biliyorum.					
27	İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.					
28	Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı biliyorum.					
29	USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.					
30	Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.					
31	Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.					
32	Kişisel mahremiyet nedir biliyorum.					
33	Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.					
34	Mavidiş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.					

	Örgütsel İletişim Envanteri'nin (Tuna, 2008) Standardizasyon İşlemleri Gerçekleştirilmiş Hali	**Asla**	**Nadiren**	**Bazen**	**Sık sık**	**Sürekli olarak**
1	Çalışanlar arasında yüz yüze iletişim imkânları fazladır.					
2	Herhangi bir probleminiz olduğunda fark edilir ve yardım edilir					
3	Kişilerin kendilerini ilgilendiren konularda fikri alınır.					
4	Yapılması gereken isler ilgili kişilere yazılı olarak iletilir.					
5	Tüm çalışanlar kurumla ilgili gelişmelerden hemen haberdar edilir.					
6	Doğum günü parti gibi resmi olmayan toplantılarda çalıştığım kuruma ilişkin edindiğim bilgiler resmi kanallardan (yazılı iletileri, kurum mailleri resmi yazışmalar gibi) elde ettiğim bilgiden daha fazladır.					
7	Herkesin yaptığı isle ilgili yetki ve sorumlulukları yazılı olarak belirlenmiştir.					
8	Bilgilendirme amaçlı iletişim araçları (gazete, yazılı genelgeler, duyurular, raporlar, ilan tahtaları, anons ve radyo sistemi) sürekli kullanılmaktadır					
9	Çalışanlar ve yöneticilerin mesai dışında da görüşme imkânı bulunmaktadır.					
10	Yapılacak is ile ilgili istenenler doğrudan o isi yapacak kişiye değil üst makamına iletilir.					
11	Çalışanlara olan kızgınlık ifadesi doğrudan sözel olarak ifade edilir.					
12	Çalışanlar arasında iyi bir bilgi alışverişi bulunmaktadır					
13	Değişik statü ve kademeye sahip bireylerin oluşturduğu çalışma grupları bulunmaktadır.					
14	Çalışanların doğum günleri evlilik yıldönümleri gibi özel günleri hatırlanır.					
15	Yöneticiler çalışanların performansları ile ilgili yeterli bilgiye sahiptir					
16	Yeni ise başlayanlar is ortamına kısa sürede alışırlar.					

	Bilgi Paylaşım Ölçeği (Aslan, 2014)	**Kesinlikle Katılmıyorum**	**Katılmıyorum**	**Kararsızım**	**Katılıyorum**	**Kesinlikle Katılıyorum**
1	Bu işyerinde çalışanlar, genellikle rapor ve resmi dokümanları diğer çalışanlarla paylaşır.					
2	Bu işyerinde çalışanlar, genellikle kendi hazırladıkları raporları ve dokümanları diğer çalışanlarla paylaşır.					
3	Bu işyerinde çalışanlar, genellikle diğer çalışanlardan raporları ve resmi dokümanları toplar.					
4	Bu işyerinde çalışanlar, genellikle bilgi paylaşımı için teşvik edilir.					
5	Bu işyerinde çalışanlar, tecrübelerini diğerleriyle paylaşır.					
6	Bu işyerinde çalışanlar, genellikle diğer çalışanların tecrübelerine ilişkin bilgileri toplar.					
7	Bu işyerinde çalışanlar, genellikle birbirlerine ilişkin bilgileri paylaşır.					
8	Bu işyerinde çalışanlar, genellikle birbirlerine ilişkin bilgileri toplar.					
9	Bu işyerinde çalışanlar, genellikle kendi uzmanlık alanları ile ilgili bilgileri paylaşır.					
10	Bu işyerinde çalışanlar, genellikle diğerlerinin uzmanlık alanlarına dayalı bilgileri toplar.					
11	Bu işyerinde çalışanlar, geçmişteki hatalardan çıkardığı dersleri gerekirse birbirleriyle paylaşır.					

Zaman ayırıp doldurduğunuz için teşekkür ederim.