BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENTÜSÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI
YÖNETİM BİLİŞİM SİSTEMLERİ TEZLİ YÜKSEK LİSANS PROGRAMI

UZAKTAN VEYA HİBRİT ÇALIŞMA MODELİNDE ÇALIŞANLARIN BİLGİ GÜVENLİĞİ DAVRANIŞLARI

HAZIRLAYAN

ELİF TÖZEN

YÜKSEK LİSANS TEZİ

TEZ DANIŞMANI

DOÇ. DR. ESMA ERGÜNER ÖZKOÇ

ANKARA – 2024

BAŞKENT ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

Tarih: 24 /06 / 2024

Öğrencinin Adı, Soyadı: Elif TÖZEN

Öğrencinin Numarası: 22110372

Anabilim Dalı: Yönetim Bilişim Sistemleri Anabilim Dalı

Programı: Yönetim Bilişim Sistemleri Tezli Yüksek Lisans Programı

Danışmanın Unvanı/Adı, Soyadı: Doç. Dr. Esma ERGÜNER ÖZKOÇ

Tez Başlığı: Uzaktan veya Hibrit Çalışma Modelinde Çalışanların Bilgi Güvenliği Davranışları

Yukarıda başlığı belirtilen Yüksek Lisans/Doktora tez çalışmamın; Giriş, Ana Bölümler ve Sonuç Bölümünden oluşan, toplam 50 sayfalık kısmına ilişkin, 31 / 05 / 2024 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 7'dir. Uygulanan filtrelemeler:

1. Kaynakça hariç
2. Alıntılar hariç
3. Beş (5) kelimeden daha az örtüşme içeren metin kısımları hariç

"Başkent Üniversitesi Enstitüleri Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Usul ve Esaslarını" inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Öğrenci İmzası:

ONAY

Tarih: 24/06/2024

Doç. Dr. Esma ERGÜNER ÖZKOÇ

TEŞEKKÜR

Bu çalışmanın hazırlanmasında;

Öncelikle, tez çalışmam boyunca bana rehberlik eden danışmanım Sn. Esma Ergüner ÖZKOÇ'a en derin teşekkürlerimi sunmak istiyorum. Onun değerli rehberliği, sarsılmaz desteği ve içten geri bildirimleri bu tezin tamamlanmasında çok büyük bir rol oynamıştır. Kendisinin uzmanlığı ve cesaretlendirmesi akademik yolculuğumu büyük ölçüde desteklemiştir.

Her zaman bana inanan ve her zorlukta yanımda olan annem Lale Yıldırıma en içten teşekkürlerimi sunuyorum. Onun sevgisi, fedakarlıkları ve sürekli desteği benim en büyük güç ve motivasyon kaynağım olmuştur. Onun varlığı olmadan bunların hiçbiri mümkün olmazdı.

Bu süreç boyunca bana hep inanan arkadaşlarıma motivasyonları için ayrıca teşekkür etmek istiyorum.

Hepinize, kalbimin en derininden teşekkür ediyorum. Desteğiniz, cesaretiniz ve bana olan inancınız bu başarıyı mümkün kıldı.

ÖZET

Elif TÖZEN, Uzaktan Veya Hibrit Çalışma Modelinde Çalışanların Bilgi Güvenliği Davranışları, Başkent Üniversitesi, Sosyal Bilimler Entüsüsü, Yönetim Bilişim Sistemleri Tezli Yüksek Lisans Programı, 2024

Son yıllarda internet, bilgisayar akıllı telefon ve elektronik cihazlar gibi dijital teknolojiler, tüm sektörlerin dönüşmesine ve işletme organizasyonlarında değişiklikler yapılmasına neden olmuştur. Covid-19 ile birlikte ülkemizde ve dünyada artan dijitalleşme ihtiyacı, özelikle bilişim başta olmak üzere bütün sektörlerdeki işletmelerin uzaktan veya hibrit çalışma sistemlerine geçmesi ile yeni bir dönem başlatmıştır. Çalışanların uzaktan veya hibrit çalışma modelini benimseme süreci, ek bilgi güvenliği tehditlerini de beraberinde getirmiştir. Bu çalışmanın temel amacı, uzaktan veya hibrit çalışanların bilgi güvenliği davranışlarını belirlemeye olanak tanıyacak bir ölçme aracının Türkiye uyarlamasını yapmaktır. Araştırmada uzaktan veya hibrit çalışanların bilgi güvenliği davranışlarının: şifre yönetimi, altyapı güvenlik yönetimi, e-posta yönetimi, kurumsal güvenlik politikası, kurumsal destek ve eğitim ve güvenlik algısına göre belirlenmesi amaçlanmıştır. Bu amaçla gerçekleştirilen çalışmaya Ankara ilinde yaşayan uzaktan veya hibrit çalışma modelinde çalışan 320 kişi katılmıştır. Ölçeğin yapı geçerliliği yapısal eşitlik modellemesi ile faktör analizi yapılarak test edilmiştir. Analizler uyarlanan ölçeğin Türkiye'de uzaktan veya hibrit çalışanların bilgi güvenliği davranışlarının değerlendirilmesi için geçerli ve güvenilir bir araç olduğunu göstermektedir.

Sonuçlar, özellikle eğitim düzeyi ve yaşın bilgi güvenliği farkındalığı üzerinde belirgin bir etkisi olduğunu ortaya koymaktadır. Uzaktan çalışanların Hibrit çalışanlara göre bilgi güvenliği davranışı konusunda daha bilinçli olduğunu göstermektedir. Yüksek lisans mezunları, ön lisans mezunlarına kıyasla daha yüksek bir farkındalığa sahiptir. Ayrıca, 38-44 yaş grubundaki bireyler, 45-50 yaş grubuna göre bilgi güvenliği konusunda daha bilinçlidir. Araştırma genel olarak çalışanların bilgi güvenliği farkındalık düzeylerinin yüksek olduğunu, ancak bazı demografik faktörlere bağlı olarak değişiklik gösterdiğini göstermektedir.

Bu çalışma elde edilen bulgular, bilgi güvenliği farkındalığını artırmak için eğitim ve politika geliştirilmesinin önemine dikkat çekmektedir. Sektör bazında farkındalık

programlarının ve güvenlik önlemlerinin uygulanması güncellemesi gerekliliği de vurgulanmaktadır. Bu bağlamda, gerçekleştirilen tez çalışmasında, işletmeler ve politika yapıcılar için bilgi güvenliği farkındalığını artırma ve güvenli davranışları teşvik etme açısından değerli çıkarımlar sunmaktadır.

Anahtar Kelimeler: Uzaktan Çalışma, Bilgi Güvenliği, Kurumsal Bilgi Güvenliği, Bilgi Güvenliği Davranışı, Çalışan Davranışı

ABSTRACT

Elif TÖZEN, Information Security Behaviors of Employees in Remote or Hybrid Working Model, Başkent University, Institute of Social Sciences, Management Information Systems Master's Program with Thesis, 2024

In recent years, digital technologies such as the internet, computers, smartphones, and electronic devices have led to the transformation of all sectors and necessitated changes in business organizations. The increased need for digitalization, especially with the onset of Covid-19, has ushered in a new era as businesses across all sectors, particularly in information technology, have transitioned to remote or hybrid working models. The process of employees adopting remote or hybrid working models has also brought additional information security threats.

The primary aim of this study is to adapt a measurement tool to the Turkish context that will enable the assessment of information security behaviors of remote or hybrid workers. The research aims to determine the information security behaviors of remote or hybrid workers based on password management, infrastructure security management, email management, corporate security policy, corporate support and training, and security perception. A total of 320 individuals residing in Ankara who work in a remote or hybrid model participated in this study. The construct validity of the scale was tested through factor analysis using structural equation modeling. The analyses indicate that the adapted scale is a valid and reliable tool for evaluating the information security behaviors of remote or hybrid workers in Turkey.

The results particularly reveal that educational level and age have a significant impact on information security awareness. Remote workers are shown to be more conscious of information security behavior compared to hybrid workers. Master's degree graduates have higher awareness compared to associate degree graduates. Furthermore, individuals aged 38-44 are more conscious of information security than those aged 45-50. The research generally shows that the level of information security awareness among employees is high, but it varies depending on certain demographic factors.

The findings of this study highlight the importance of developing education and policies to enhance information security awareness. The necessity of updating sector-specific awareness programs and security measures is also emphasized. In this context, the thesis study provides valuable insights for businesses and policymakers in terms of increasing information security awareness and promoting secure behaviors.

Keywords: Remote Work, Information Security, Corporate Information Security, Information Security Behavior, Employee Behavior

İÇİNDEKİLER

TABLOLAR LİSTESİ

Sayfa

ŞEKİLLLER LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR LİSTESİ

BGYS	: Bilgi Güvenliği Yönetim Sistemi
BT	: Bilgi Teknolojisi
EDR	: Endpoint Detection and Response
EM	: Email Management
IBM	: International Business Machines Corporation
ISM	: Infrastructure Security Management
MFA	: Çok Faktörlü Kimlik Doğrulama
OSP	: Organizasyonel Security Policy
PM	: Pasaport Management
POS	: Perception of Security
SPSS	: Statistical Package for the Social Sciences
TM	: The Thinging Machine
UML	: Unified Modeling Language
VPN	: Virtual Private Network

1. GİRİŞ

Geçmişten günümüze yaşanan teknolojik ve bilimsel ilerlemeler, savaşlar, toplumsal salgınlar gibi küresel etkiye sahip olaylar bilgi güvenliği konusunda, uzmanların yeni zorluklar ve tehditlerle karşılaşmasına sebep olmuştur. Dünyayı hızla dijitale dönüştüren küresel salgın COVID-19 ile birlikte uzaktan çalışma kavramı, birçok şirket ve kuruluş için daha yaygın hale gelmiştir. Pandemi sırasında, birçok işletme, hükümet ve kuruluş, çalışanlarını uzaktan çalışma modeline geçirmek zorunda kalmıştır. Ancak bu geçiş sadece bir zorunluluktan ibaret olmamıştır; Birçok işletme uzaktan çalışmanın avantajlarını görmüş ve bu modeli devam ettirmiştir. Uzaktan çalışma, işin tamamının ya da bir kısmının, alışılmış çalışma alanı dışında, farklı bir mekânda yapılması anlamına gelir. (Ogbanuge ve diğer., 2023). Uzaktan ve hibrit çalışmanın kurumlar açısından en önemli avantajlarından biri yerel bağımsızlığa sahip daha ucuz işçileri istihdam edebilmeleridir. Aynı zamanda çalışanlara da zaman tasarrufu açısından fayda ve avantajlar sağlamaktadır (Alagöz ve Allahverdi ,2011). Buna ek olarak, engelli bireyler gibi çalışma hayatında dezavantajlı gruplar, bu sisteme rahatça uyum sağlayabilmektedir. Bu durum, işletmelerin en uygun çalışanları bulmasını kolaylaştırırken, maliyet açısından da fayda sağlamaktadır (Şakar ve Şahin, 2021). Bunların yanı sıra işletmeler bu çalışma modeli ile ofis alanı ve altyapı maliyetlerinden de tasarruf sağlamıştır. Uzaktan çalışma modeli bu avantajların yanı sıra iletişim ve iş birliği araçlarının da gelişmesine katkıda bulunmuştur (Bodepudi ve Reddy, 2021). Çeşitli sanal toplantı, anlık mesajlaşma ve dosya paylaşım yazılımları uzaktan çalışmayı daha etkili hale getirmiştir. İşletmeler için dijitalleşme, sadece veri ve kaynakların dijitalleşmesi değil aynı zamanda süreçlerin, algının ve yönetimin de dijitalleşmesi anlamına gelmiştir (Uçar ve Tutgaç, 2022). Bu durum işletmelerde çalışanların eğitilmesi ve çalışma süreçlerinin optimize edilmesi ihtiyacını doğurmuştur.

Uzaktan veya hibrit çalışma modelleri, iş dünyasında giderek daha yaygın hale gelmektedir ve bu modellerin benimsenmesi, bilgi güvenliği alanında yeni ve önemli zorluklar ortaya çıkarmaktadır. Bu bağlamda, çalışanların bilgi güvenliği davranışları üzerine yapılan araştırmalar, hem işletmelerin veri güvenliğini sağlama stratejilerini anlamak hem de uygun önlemleri alabilmek için kritik öneme sahiptir. Uzaktan veya hibrit çalışma modeline geçiş, çalışanların işyeri dışında bilgiye erişimini artırarak, güvenlik risklerini artırabilir. Bu durum, çalışanların bilgi güvenliği politikalarına uyumunu ve risk

farkındalığını daha da önemli hale getirir. Dolayısıyla, bu alandaki araştırmalar, işletmelerin bilgi güvenliği stratejilerini güçlendirmek ve uzaktan çalışma ortamında veri güvenliğini sağlamak için kritik bir bilgi kaynağıdır.

Uzaktan çalışmanın yaygınlaşmasıyla birlikte kişisel ve kurumsal cihazlara, herhangi bir güvenlik katmanı yapısına sahip olmayan ev internet ağlarına, mobil uygulamalara vb. yönelik siber saldırı girişimleri katlanarak arttırmıştır (Koyuncu, 2021). Zira bilgi, bilgi yönetimi ve bilgi teknolojisi (BT), işletmelerin en kritik öneme sahip kaynaklarıdır. Bu nedenle işletmelerin bilgi sistemleri güvenliğine ilişkin politikalara öncelik vermesi gerekmiştir (Gülmüş, 2010).

Günümüzde, bilgi sistemlerinin küreselleşmesi sonucunda doğrudan veya dolaylı yönden ilişkili olan ve bu sistemleri kullanan tüm birey ve kurumların artık bilgi güvenliğine daha fazla katkıda bulunması gerekmektedir (Zhen ve diğer., 2022). Internet'in yaygın olarak kullanılması ve internet üzerinde kullanılan çevrimiçi uygulamalardaki artış, güvenlik açıklarının da artışına sebep olmuştur. Bu sebeple bilgi güvenliğini sağlamak sadece işletmelerin bilgi güvenliği politikası sorumluluğunda değil aynı zamanda çalışanların da sorumluluğu olmaya başlamıştır (Yel ve Atasoy, 2021). Dijitalleşme çağında bilgi toplumunda bilgi güvenliğinin ve bilgi altyapısının sağlanması dikkatli edilmesi gereken önemli bir konudur (Yalçın ve Beril, 2021).

Bu tez çalışmasının amacı uzaktan veya hibrit çalışma modellerinde faaliyet gösteren işletme çalışanlarının bilgi güvenliği davranışlarını araştırmaktır. Çalışmada Saeed (2023) tarafından geliştirilen ölçek temel alınarak Türkçeye uyarlanmıştır. Bu kapsamda şifre yönetimi, altyapı güvenlik yönetimi, e-posta yönetimi, kurumsal güvenlik politikaları, kurumsal destek ve eğitim güvenliği düzeyi algısı bilgi güvenliği davranışının alt boyutları olarak belirlenmiştir. Elde edilen verilerle uzaktan veya hibrit çalışma modelindeki çalışanların güvenlik davranışları incelenerek çalışılan sektör, eğitim düzeyi, cinsiyet gibi faktörlere göre sonuçlar değerlendirilmiştir.

1.1. Bilgi Güvenliği ve Uzaktan Çalışma

1.1.1. Bilgi Kavramı

Veri, olayların ve nesnelerin özelliklerini temsil eden semboller olarak kabul edilir. Bu semboller, işlenmemiş yani ham haldeyken tek başlarına bir anlam ifade etmezler (Ackoff, 1989: 4; Bellinger, Castro ve Mills, 2004: 1). İşlenmemiş veriler, kullanım durumuna bakılmaksızın herhangi bir formatta olabilir ve anlamsızdır; ancak bilginin ve enformasyonun oluşturulmasında temel bir rol oynarlar (Yılmaz, 2009: 4). Enformasyon, işlenmiş veri kümeleridir ve bu işleme süreci, elde edilen verilerin kullanılışlığının arttırılmasını amaçlamaktadır. Enformasyon, nesnelerin ve olayların özelliklerini anlamlı ve kullanışlı bir şekilde sunar. Enformasyon kimin, neyi, ne zaman, nerede ve nasıl yaptığına ilişkin bilgiler içerir (Ackoff, 1989: 4). Ayrıca enformasyon, olayları ve nesneleri yeni bir perspektiften değerlendirilmesini mümkün kılmıştır, böylece daha önce fark edilmeyen anlamların ve beklenmedik ilişkilerin ortaya çıkarılmasına yardımcı olmuştur. Bu nedenle, enformasyon bilginin keşfedilmesi ve oluşturulması için zorunlu bir araçtır (Nonaka ve Takeuchi, 1995: 58). Bilgi ise, genel olarak derinlemesine işlenmiş enformasyon olarak kabul edilir, ancak bu tanım yeterli değildir (Gurteen, 1999: 1). Bilgi, bireyin inanç ve değerleriyle şekillenen enformasyon akışından türetilir (Nonaka ve Takeuchi, 1995: 59). Bu çerçevede, bilgi deneyim, tecrübe ve yorumun birleşimi ile oluşan kişisel olarak düzenlenmiş enformasyon olarak ifade edilmiştir (Aktan ve Vural, 2016: 8). Bilgi, sadece enformasyondan ayrılmakla kalmaz, aynı zamanda bilginin eyleme dönüşebilme kapasitesiyle de özdeşleştirilir (Nonaka ve Takeuchi, 1995: 46; Liebowitz ve Megbolugbe, 2003: 190). Polanyi'nin (1966, Aktaran: Akgün ve diğer., 2009: 22) belirttiği üzere, bilgi açık ve örtük olmak üzere iki farklı kategoride incelenebilir, her ikisi de kendi içinde ayrı ayrı değerlendirilmiştir. Bilgi, kişinin gerçeklikle bilişsel temas halinde olduğu oldukça değerli bir durumdur. (Zagzebski, 2017). Bilgi olgusu zaman içinde birbirinin üstüne koyarak çok yönlü bir şekilde evrimleşmiştir. Bilgiye ulaşma ve paylaşma süreçleri, tarih boyunca kültürler arası etkileşim, teknolojik gelişmeler ve sosyal değişimlerle şekillenmiştir. Bu nedenle, bilginin ortaya çıkışı sürekli bir evrimin ürünüdür (Daston, 2017). Bilginin günümüzde insanlık adına teknolojilerin gelişmesi ile doğru orantıda ilerlemektedir ve bu bilgilerin şahıs veya işletmelerin saklaması, güvenliğini sağlaması gerekmektedir söz konusu bu güvenlik olmadığında kötü amaçlı kişilerin eline geçtiğinde çok büyük maddi manevi sonuçlar doğurabilmektedir (Şanlısoy, 2016).

1.1.2. Bilgi Güvenliği

Bilgi güvenliği genellikle bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasını ifade eder. Başka bir deyişle, bilginin izinsiz erişime, kullanımına, ifşa edilmeye, değiştirilmeye, bozulmaya ve yok edilmeye karşı korunmasıdır (Ecek ve Çakmak, 2022).

Yıllar geçtikçe bilgi güvenliği, değişen teknolojilere, tehditlere ve dijital verilerin artan önemine yanıt olarak gelişmiştir. Bilgisayar öncesi dönemde bilgi güvenliğinin tarihçesini ele alırsak, başlangıçta, bilgi güvenliği, kâğıt belgelerin güvenliğinin sağlanması ve binaların güvenliğinin sağlanması gibi fiziksel güvenliğe odaklanmıştı (Gülmüş, 2010).

Bilgiyi iletim, işlem ve depolama süreçlerinde koruma ihtiyacı, bilgi teknolojilerinin kullanımının yaygınlaşması ve bilginin işletmeler için kritik bir kaynak olarak kabul edilmesiyle daha da önem kazanmıştır (Dlamini, Eloff ve Eloff, 2008: 189; Xu, Wang ve Yan, 2021: 1). Bu durum, yeni ve daha karmaşık güvenlik tehditlerini de beraberinde getirmiştir (Eloff ve Eloff, 2005: 10). Bilgi güvenliği tarihine bakıldığında, bu alanın bilgisayar güvenliği ile yakından ilişkili olduğu görülür (Whitman ve Mattord, 2011: 4). İlk ana bilgisayarların 2. Dünya Savaşı sırasında geliştirildiği ve bu bilgisayarların iletişim kodlarını çözmek amacıyla kullanıldığı dönemde, bilgisayar güvenliğinin önemi ortaya çıkmıştır (Whitman ve Mattord, 2011: 5). O dönemdeki temel güvenlik odakları, bilgisayarlara yetkisiz erişimin önlenmesi ve cihazların çalınma ya da zarar görme risklerinin azaltılmasıydı (Dlamini ve diğer., 2008: 190). Bu dönemde, cihazların ve onların sunduğu hizmetlerin korunması için çeşitli güvenlik katmanları devreye sokulmuştur (Whitman ve Mattord, 2011: 5).

1990'lı yılların sonlarına doğru saldırganların taktikleri solucan ve virüslerden daha sofistike saldırılara evirilmiş, e-postalara ve web sitelerine kötü amaçlı yazılım eklemek gibi yöntemler kullanılmaya başlanmıştır. Bu tehditlere karşı önlem olarak güvenlik duvarları kullanılmaya başlanmış ancak internet kullanılmasının artması bu önlemleri yetersiz hale getirmiştir. Hacker toplulukları geniş kitlelerin erişimine açık hale gelen hacking araçlarıyla bu alanda yeni bir dönem başlatmıştır. Bilişim teknolojilerinin yaygınlaşması ve mobil cihazların kullanımının artması ile birlikte 21. yüzyılda saldırı yöntemleri de gelişmiş, saldırganlar finansal kazanç sağlama amacıyla hackleme gibi

yöntemlere yönelmiştir (Dlamini ve diğer., 2008: 192). Bilişim teknolojilerindeki sürekli gelişme, yeni güvenlik tehditlerinin ortaya çıkması riskini de beraberinde getirmektedir. Bu bağlamda bilgi güvenliğinin sağlanabilmesi amacıyla fiziksel güvenlik, güvenlik farkındalığı, kimlik yönetimi ve çevre güvenliği gibi konulara dikkat edilmesi gerekmektedir (Dlamini ve diğer., 2008: 192).

Rusyada 2022 yılında yapılan çalışmada uzaktan çalışma alanında bilgi güvenliğinin sağlanmasına ilişkin sorunlar ele alınmaktadır. Korona virüs salgını nedeniyle kısıtlayıcı tedbirler ve personelin uzaktan çalışma modeline geçirilmesi sırasındaki bilgi güvenliği sorunları incelenmiştir. Çalışmada, kuruluşun bilgi güvenliğinden sorumlu uzmanların, ofisteki iş istasyonlarında güvenliğin sağlandığı tüm teknik araç ve politika cephaneliğini uygulama fırsatına sahip olmaması nedeniyle, uzaktan çalışanlar aracılığıyla bilgi sızıntısı tehdidi nispeten daha yüksek olduğu sonucuna ulaşılmıştır. Bilgi sızıntısı ciddi sorunlara yol açacağından, işletmelerin bilgi güvenliğini sağlamak için hangi araçları kullanabileceğinin planlanmasının önemli olduğu vurgulanmaktadır (Kolomoets 2022).

Bilgi güvenliği üzerine yapılan araştırmaların bazıları da uzaktan eğitim alan öğrenciler üzerine yapılmıştır (Çakmak Karapınar ve Daş, 2023) (Karaoğlan Yılmaz ve diğer., 2014). Öğrencilerin Bilgi güvenliği konusundaki farkındalıkları incelendiğinde öğrencilerin çoğunun bilgi güvenliği konusunda temel bilgi eksiklikleri olduğu görülmüştür. Özellikle, güçlü şifre kullanımı, çevrimiçi hesapların korunması ve güvenli internet kullanımı gibi temel bilgi güvenliği prensiplerine ilişkin bilgi seviyelerinin düşük olduğu belirtilmiştir. Araştırmalar sonucunda öğrencilere bilgi güvenliği konusunda düzenli eğitimlerin verilmesinin önemi belirtilmiş ve bilgi güvenliği politikalarının etkin bir şekilde iletilmesinin gerekliliğine işaret edilmiştir. Öte yandan Gültekin ve Özal tarafından 2023 yılında öğrencilerinin bilgi güvenliği farkındalığı üzerine odaklanan diğer bir çalışmada, öğrencilerin çoğu temel bilgi güvenliği kavramlarına hâkim olduğunu, ancak günlük uygulamalarında güvenlik önlemlerini yeterince uygulamadığını göstermiştir (Gültekin ve Özal, 2023).

1.1.2.1. Bilgi güvenliği unsurları

Bilgi güvenliği literatüründe bilgi güvenliğini sağlamak için üç temek unsur açıklanmaktadır; Gizlilik bütünlük ve kullanılabilirlik özelliklerinin önemine vurgu yapar

(Vural, 2007: 40; Stamp, 2011: 2; Whitman ve Mattord, 2011: 14; Andress, 2014: 6). Bu temel özellikler detaylı bir şekilde ele alınmıştır (Whitman ve Mattord, 2011: 14).

Gizlilik:

Gizlilik, yetkisiz kişilerin verilere erişimini engelleme uygulaması olarak açıklanabilir (Stamp, 2011: 2; Andress, 2014: 6). Bu, ilgili bilgiye yalnızca erişim haklarına sahip bireylerin erişebilmesini sağlar (Whitman ve Mattord, 2011: 15). Elektronik verilerin yetkisiz kişiler tarafından ele geçirildiği takdirde anlamını yitirmesi, gizliliğin bir parçasıdır (Vural, 2007: 40). Dizüstü bilgisayarın kaybedilmesi, omuzdan bakılarak (shoulder surfing) şifrenin çalınması, yanlış kişiye gönderilen e-posta ekleri, sosyal mühendislik yoluyla elde edilen bilgiler veya sistemimize sızan saldırganlar gizlilik için potansiyel tehditlerdir (Andress, 2014: 6; Grama, 2020: 14). Gizliliğin koruması için bilgilerin sınıflandırılması, şifreleme, erişim kontrolleri, güvenli belge depolama, güvenlik politikalarının uygulanması ve eğitimler gibi önlemler alınabilir (Grama, 2020: 36; Whitman ve Mattord, 2011: 15). Gizlilik, diğer bilgi güvenliği özellikleriyle entegredir ve mahremiyetle doğrudan ilişkilidir (Whitman ve Mattord, 2011: 15).

Bütünlük:

Bütünlük, verilerin istenmeyen ya da yetkisiz değişikliklerden koruma kapasitesi olarak ifade edilebilir (Andress, 2014: 6). Veri bütünlüğü, bilginin doğru, eksiksiz ve bozulmadan kalması anlamına gelir (Whitman ve Mattord, 2011: 16). Verilerin yetkisiz bir şekilde değiştirilmesi, silinmesi ya da yetkilendirilmiş ancak değişiklikler bütünlüğün bozulmasına yol açar (Andress, 2014: 6; Grama, 2020: 37). Bilginin depolanması veya iletilmesi sırasında meydana gelebilecek bozulmalar da bütünlüğü tehlikeye atar (Whitman ve Mattord, 2011: 16). Bütünlüğün korunması için sadece yetkisiz değişiklikleri önlemeye yönelik araçlar yeterli değildir aynı zamanda gerektiğinde izin verilen değişikliklerin geri alınabilmesi de önemlidir (Andress, 2014: 6). Güvenlik denetimleri ve antivirüs programları, bilginin bütünlüğünün sağlanması etkilidir (Grama, 2020: 37).

Erişilebilirlik –Kullanılabilirlik

Erişilebilirlik, kullanıcıların ihtiyaç duydukları anda bilgiye ulaşabilmesidir. (Andress, 2014: 6). Bubilgilerin yetkili kullanıcılara hızlı ve güvenilir bir şekilde ulaşmasını sağlar (Vural, 2007: 41; Grama, 2020: 39). Erişilebilirlik, sistem kesintileri ve arızaları sonrasında hızlı iyileşme, birden fazla arıza noktasında bulunması durumunda yedek ekipmanların bulunabilirliği gibi önlemlerle desteklenebilir. (Grama, 2020: 39).

Hristova ve arkadaşları 2021 yılında, Birleşik Krallık çalışanlarının karantinanın seyrinde evden çalışanların eğitilmesi ve iş süreçlerinin optimize edilmesi ihtiyacını vurgulamıştır. Uzaktan çalışma ortamında bilgi güvenliğinin kritik bir konu olduğu belirtilmiş ve bilgi güvenliğinin yalnızca yetkisiz erişimden korunmayı değil, aynı zamanda bilgilerin ifşa, bozulma, değiştirme, denetleme, kaydetme veya imha edilmesini önleme uygulaması olması gerekliliğine değinilmiştir. Bilginin işletmeler için hayati önem taşıdığı ve bilgi güvenliğinin temelinde bilgi güvencesi olduğu vurgulanmıştır. Ayrıca, makale belediye yönetimi için kritik bilgilerin ne olduğunu ve bunların nasıl sınıflandırılabileceğini standartlar ve direktiflerle tanımlanmıştır (P. Hristova, R. Rusev, B. Ivanova 2021).

Etkili Şifre Yönetimi

Şifre yönetimi güvenli kullanım davranışını teşvik etmek için önemli bir kriterdir. Şifre yönetimi bireylerin ve kuruluşların güvenliklerini sağlamak için kullandıkları önemli bir uygulamadır. Uygun bir şifre yönetimi stratejisi benimsemek, olumsuz etkileri önleyebilir ve güvenliği artırabilir.

Doğan ve Aşan (2016) tarafından yapılan bir araştırmaya göre bireylerin şifre yapıları üzerine yapılan çalışmada İncelenen şifrelerin uzunlukları makul olmasına rağmen tahmin edilebilir kişisel bilgilerden oluşan ve bir kullanıcı tarafından belirlenen şifrelerin genellikle az sayıda karakter grubu kullandığı tespit edilmiştir (Doğan ve Aşan, 2016).

Tam, Glassman ve Vandenwauver (2010) şifre yönetiminin psikolojisini inceledikleri çalışmalarında güvenlik ile kullanım kolaylığı arasındaki ilişkiyi ele almışlardır. Güvenlik farkındalığı programlarının kullanıcılara önleyici bir bilgi güvenliği kültürü geliştirmede

nasıl yardımcı olabileceği tartışılmıştır. Şifre yönetimi konusunda bir güvenlik farkındalığı çalışması yürütmüşlerdir ve katılımcı öğrencilerin güvenlik sorunlarının farkında olmalarına rağmen yine de uygun şifre yönetimini uygulamayı reddettiklerini bulmuşlardır. Mesela öğrenciler şifre paylaşmanın riskli olduğunu bilmelerine rağmen neredeyse yarısı şifrelilerini paylaşmışlardır. Ayrıca öğrencilerin eğitim seviyelerinde ilerleme oldukça daha güçlü şifreler kullanma eğiliminde olduklarını da bulmuşlardır.

Altyapı Güvenlik Yönetimi

Altyapı güvenlik yönetimi, bir organizasyonun teknolojik altyapısının güvenliğini korumak ve sürdürmek için gerekli stratejilerin belirlenmesi, uygulanması ve sürekli olarak güncellenmesini sağlayan kapsamlı bir yönetim yaklaşımıdır (Jain, Sinha, Agrawal ve Yadav 2022). Siber güvenlik, dijital altyapının saldırılara, tehditlere ve zayıflıklara karşı algılanmasıdır. Siber suç herhangi bir zamanda herhangi bir yerden gelebilir ve ciddi sonuçlara yol açabilir (Karabacak ve Özkan 2010). Yalnızca teknik risklerin değil kurumsal, fiziksel, süreçsel ve personel kaynaklı ilgili riskleri de dikkate alan önerilen süreç tabanlı risk analizi yöntemi, sadece bilgi teknolojileri departmanının sorumluluğundaki teknik risklere odaklanan bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulumunun beklenen etkiyi göstermeyeceğini ortaya konulmalıdır.

Gurung, Luo ve Liao (2009) casus yazılımlara karşı harekete geçme motivasyonlarını inceleyerek önemli bir çalışma yürütmüşlerdir. Casus yazılım önleme araçlarının tüketicilerin siber saldırılara karşı korunmasına yardımcı olduğunu vurgulamıştır.

Anna Georgiadou ve arkadaşları 2021 yılında COVID-19 salgını nedeniyle uzaktan çalışmanın yaygınlaşmasıyla birlikte farklı ülkeler ve sektörlerdeki kuruluşların siber güvenlik kültürünü değerlendirmeyi amaçlamıştır. 13 Avrupa ülkesinden 264 katılımcının yer aldığı araştırmada web tabanlı anket aracılığı ile veri toplanmıştır. Katılımcıların %53'ü, salgın sırasında işverenlerinden evden çalışmaya ilişkin herhangi bir güvenlik talimatı almadıklarını belirtmiştir. Sonuç olarak evden çalışmak için kullanılan donanımların çoğu güvenlik politikalarına uygun olmadıkları ve insan faktörünün bilgi güvenliği ilerlemesinde temel bir rol oynadığı ve daha fazla araştırma gerektirdiği vurgulanmıştır (Anna Georgiadou , Spiros Mouzakitis, Dimitris Askounis 2021).

Koushik, Chandrashekhar ve Takkalakaki (2015), bilgi güvenliği tehditleri, farkındalık ve bilinç üzerine yaptıkları araştırmalarında önemli bulgular elde etmişlerdir. Kullanıcıların, yalnızca kilitli ekran koruyucu olsa bile ofisten çıktıktan sonra bilgisayarlarından uzaklaşırken ekran kilitleme uygulamasını benimsemelerini gerektiğini önerilmiştir.

E-Posta Güvenliği Yönetimi

E-posta güvenliği yönetimi, bir organizasyonun veya bireyin e-posta iletişimlerinin güvenliğini sağlamak için takip edilen süreçler ve uygulamalar bütünüdür. Bu, kötü niyetli saldırılara veri sızıntılarına ve diğer güvenlik tehditlerine karşı korunmayı amaçlamaktadır.

Alqahtani (2022), yazılım ve e-posta güvenliği üzerine yapılan bir çalışmaya dayanarak siber güvenlik farkındalığını ele alan bir rapor sunmaktadır. Bu çalışmada, İmam Abdulrahman Bin Faysal Üniversitesi öğrencilerinin siber güvenlik farkındalıkları incelenerek ve yazılım güvenliği ile e-posta güvenliği konularında yapılan çalışmaların etkisi değerlendirilmiştir. Analiz sonucunda hem yazılım güvenliği hem de e-posta güvenliği konularında bilinçlilik düzeyinin siber güvenlik farkındalığı üzerinde anlamlı bir etkisi olduğu tespit edilmiştir. Bu sonuçlar, öğrencilerin bu konularda bilinçli olduklarını ve önlemler aldıklarını göstermektedir.

Al-Fedaghi ve Alnasser (2020), e-posta sistemi üzerine bir durum çalışmasını temel alan, ağ güvenliğini modelleme konusunu ele almaktadır. Bu araştırmada, güvenlik oluşturma görevinin, korunan varlıkların bulunduğu operasyonel ortamın sistem diyagramatik bir gösterimini gerektirdiği tartışılmaktadır. Mevcut modelleme dilleri (örneğin, UML and ad hoc diagrams) eleştirilmiştir; çünkü bu diller, büyük ölçüde heterojen kavramlar veya sistematik olmayan semboller (örneğin, duvar, bulut, ekran, insan figürü vb.) içermektedir. Bunun yerine, makalede, TM (the thinging machine) modelleme ve TM dilinin gerçek bir e-postaya uygulanması önerilmektedir. Bu yaklaşım, bir e-posta akışı sırasında güvenlik hususlarını takip ederek sistemdeki çeşitli bileşenleri görsel olarak temsil etmiştir. Elde edilen harita, bir ağ mühendisi için ağ şeması ne ise, bir e-posta güvenlik görevlisi için de benzer bir araç olabilir. Gelecekteki çalışmalar, TM modelinin farklı ağ türlerine nasıl uygulanabileceğini araştırmaktır.

Eğitim Güvenlik Düzeyi Algısı:

Güvenlik eğitimi ve öğretimi, bir organizasyondaki çalışanların bilgi güvenliği konusunda farkındalığını artırmak, doğru güvenlik uygulamalarını teşvik etmek ve güvenlik risklerini azaltmak için önemli bir süreçtir. Eğitimin yanı sıra çalışanların aralarında bilgi paylaşımı kültürün geliştirmesini güvenlik açıklarına karşı kurumsal dayanıklılığı artırabilir.

Knapp, Morris Jr, Marshall ve Byrd (2009), bilgi güvenliği politikalarını oluşturmanın kuruluşlar için bir süreç modelini detaylandıran bir çalışmayı rapor etmektedir. Bilgi güvenliği politikası oluşturmanın kuruluşlar için hayati önem taşıdığını vurgulamıştır; bu nedenle kuruluşların güvenlik politikaları oluşturmasına yardımcı olmak için genel bir bilgi güvenliği politikası süreç modelini önerdiler. Bu tür genel çerçeveler küçük ve orta ölçekli işletmelerin sınırlı kaynaklarıyla temel bilgi güvenliği protokollerine sahip olmalarını sağlamak açısından daha faydalı olduğunu vurgulamışlardır.

Hart, Margheri, Paci ve Sassone (2021), siber güvenlik farkındalığı ve eğitimi için Riskio adlı ciddi bir oyunu tanıtan bir çalışma gerçekleştirmiştir. Makale, siber güvenlik risklerine karşı kuruluşların stratejilerini sürekli güncellemesi gerektiğini vurgulamaktadır. Çalışanlara yönelik eğitim kurslarıyla farkındalık yaratmanın önemli olduğu belirtilmektedir. Riskio adlı masa üstü oyunu, teknik olmayan çalışanların siber güvenlik konusundaki farkındalığını artırmayı hedeflemektedir. Çalışmanın sonuçları, oyunun etkili bir siber güvenlik eğitimi aracı olarak potansiyelini göstermektedir.

Alkhazi, B., Alshaikh, M., Alkhezi, S., ve Labbaci, H. (2022) yılında bilgi güvenliği farkındalık eğitimi yöntemlerinin bilgi, tutum ve davranış üzerindeki etkisinin değerlendirilmesi adlı çalışmada, farklı müdahale stratejilerinin çalışanların siber güvenlik önlemlerine yönelik bilgi, tutum ve davranışları üzerindeki etkisi incelenmiştir. Sonuçlar, tüm müdahale yöntemlerinin bilgi geliştirmede benzer performans sergilediğini ancak tutum, davranış ve memnuniyet açısından önemli farklılıklar olduğunu göstermektedir. Özellikle, farklı eğitim yöntemlerine katılan çalışanların, sadece derslere katılanlara göre daha olumlu tutumlar geliştirdiği görülmüştür. Ayrıca, metin tabanlı ve oyun tabanlı katılımcıların, diğerlerine göre daha iyi davranış değişikliği gösterdiği belirlenmiştir. Sonuçlar ayrıca, eğitim programının uzunluğunun algılanan etki ile ilişkili olduğunu ve

katılımcıların gelecekteki bilinçlendirme kampanyalarına katılımlarının genel eğitim deneyimlerinden etkilendiğini göstermektedir. Bu bulgular, güvenlik stresi ve yorgunluğun azaltılmasının, uygun eğitim stratejileri seçilerek sağlanabileceğini ve çalışanların daha güvenli organizasyonlara katkıda bulunabileceğini göstermektedir.

McIlwraith, A. (2021). Bilgi Güvenliği ve Çalışan Davranışı kitabında birçok ilgili konuya değişmiştir ve kitap da yer alan bölümde personelin eğitilmediği durumlarda hatalar yapmalarının şaşırtıcı olmaması gerektiği vurgulanmaktadır. Operasyon personelinize yardımcı olabileceğiniz en önemli şey iyi bir eğitim olduğu söylenmiştir. Çok az insanın aslında sorumluluklarının ne olduğunu bildiği söylenmiştir ve iyi bir eğitimin hataları azaltılacağı da vurgulanmıştır. İyi eğitim, hata sayısını azaltarak güvenliği artıracağını ve insanların neyin kendilerinden beklendiğini bildiklerinde genellikle bunu uygulayacakları anlatılmıştır.

1.1.2.2. Kurumsal bilgi güvenliği

Kurumsal bilgi güvenliği, bir kuruluşun sahip olduğu bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirlik korumak için alınan önlemleri ve uygulanan politikaları kapsar. Bu kapsamda, kurumsal bilgi güvenliği önlemleri ile bilgi varlıklarının yetkisiz erişime karşı korunması, veri kaybının önlenmesi, bilgi güvenliği politikalarının oluşturulması ve uygulanması gibi adımlar atılır. Kurumsal bilgi güvenliği, kuruluşların itibarını korumak, yasal gereksinimleri yerine getirmek ve iş sürekliliğini sağlamak için önemli bir konudur.

Kamu ve özel sektör işletmeleri için bilginin oluşturulması kadar, bu bilgilerin güvenli bir şekilde saklanması da son derece kritik bir öneme sahiptir. Bu amaçla geliştirilen ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı, kurumsal bilgi güvenliğinin sağlanmasına odaklanmaktadır.

Kurumsal bilgilerin güvenliği, kullanılan bilgi sistemlerinin zayıflıklarının erken tespiti ve hızlı bir şekilde giderilmesiyle sağlanabilir. Güvenlik zafiyetlerinin saldırı gerçekleşmeden önce tespit edilip düzeltilmesini sağlayan güvenlik testleri, kurumsal bilgi güvenliği için hayati öneme sahiptir (Vural ve Sağıroğlu 2011 :15).

Günümüz teknoloji dünyasında, kurumlar çalışanlarını zararlı yazılımlardan ve ortalama saldırılarından korumak amacıyla çeşitli internet sınırlamaları uygulamaktadır. Bu sınırlamaların temel nedeni, kurumsal bilgi güvenliğini sağlamaktır. Bununla birlikte, iç verimliliği artırmak ve kurumun itibarını korumak amacıyla da bu tür sınırlamalar yapılmaktadır (Ganal ve diğer., 2017 : 12).

Kurumlar için bilgi güvenliği giderek artan güvenlik tehditleri nedeniyle yaşamsal bir hale gelmiştir (Galvez ve Guzman, 2009: 1). Kurumların bilgi varlıklarını, donanım ve yazılımlarını yanlış ya da kötü niyetli kullanımlardan korumak kurumsal bilgi güvenliğinin temel hedefidir (Gregory, 2003: 29; Peltier, 2013: 13). Bu, yalnızca teknolojik bir mesele değil, aynı zamanda iş ve süreç yönetimi meselesi olarak ele alınmalıdır (Özcan, 2009: 47). Kurumsal bilgi güvenliğine yapılan yatırımlar, doğru stratejilerle uygulandığında, kurumun finansal ve fiziksel kaynaklarını, itibarını, hukuki duruşunu, çalışanları ile diğer somut ve soyut varlıklarını koruyarak misyonunu ve iş hedeflerini destekler (Peltier, 2013: 13). Etkin bir bilgi güvenliği yönetimi, organizasyona rekabet üstünlüğü, müşteri memnuniyeti, güvenilir bir imaj ve itibar gibi çeşitli avantajlar sağlayabilir (Cheng ve Ho, 2006: 348). Bilgi güvenliği zafiyetleri ise maddi zararlar ve kurumsal itibar kaybı gibi ciddi sonuçlara yol açabilir (Cavusoglu, Cavusoglu ve Raghunathan, 2004: 65). Risk yönetimi süreçlerinin uygulanmasıyla, karşılaşılabilecek risklerin belirlenmesi ve ardından bu risklere uygun güvenlik önlemlerinin tasarlanması gerekir (Peltier, 2013: 13). Bilgi güvenliği, birkaç önemli ilkeye dayanmalıdır (Peltier, 2013: 13):

- Bilgi güvenliği, organizasyonun misyonunu ve hedeflerini desteklemelidir.
- Güvenlik, görevlerin vazgeçilmez bir parçası olarak görülmelidir.
- Bilgi güvenliği maliyet etkin olmalıdır.
- Çalışanların ve yöneticilerin güvenlikle ilgili sorumlulukları net bir şekilde ifade edilmelidir.
- Bilgi güvenliği, bütünleşik ve kapsamlı bir yaklaşım gerektirir.
- Bilgi güvenliği, sürekli değerlendirilmeli ve zamanla değişen ihtiyaçlara uyum sağlamalıdır.
- Bilgi güvenliği, kurum kültürü ile uyumlu olmalıdır. Özellikle bilgi açısından zengin olan üniversiteler, not değişiklikleri, kişisel bilgilerin ele geçirilmesi gibi sık karşılaştıkları güvenlik riskleri nedeniyle etkin bilgi güvenliği önlemleri almalıdır (Yerby ve Floyd, 2018: 2; Rezgui ve Marks, 2008: 241).

1.1.2.3. Kurumsal bilgi güvenliği riskleri

Kurumlar, bilgi güvenliği politikalarını uygularken farklı yaklaşımlar benimseyebilirler. Bazıları tek bir politika belirlerken, diğerleri ise çeşitli konular için birden fazla politika oluşturmayı tercih edebilirler. Ancak, bu politikalar sadece bilgi güvenliği veya BT ekiplerinin sorumluluğunda değildir. Bazen sadece bu ekiplerin sorumluluğu gibi algılanır, oysaki tüm kurum çalışanlarının bilgi güvenliğine katkı sağlaması gerekir. Bu nedenle, bilgi güvenliği politikaları tüm çalışanları ilgilendirir ve onların okuması ve uygulaması gereken belgelerdir.

Eray Çek 'in 2017 yılında Kurumsal Bilgi Güvenliğinde İnsan Faktörü araştırmasında, kurumlarda etkili ve verimli bir bilgi güvenliği yönetimi için en önemli şart, üst yönetim desteği olduğu sonucuna varılmıştır. Bu destek, yönetim kurulu seviyesinde sağlanmalıdır. Üst yönetimin bilgi güvenliğine sahip çıkması, sorumluluk alması ve destek vermesi, kurumsal bilgi güvenliği yönetiminin sağlanmasında kritik bir rol oynamaktadır.

Güvenlik tehditleri, bireylerin veya kurumların ağlarını, bilgisayarlarını, yazılımlarını ve verilerini bilinçli olarak tehlikeye atma eylemleridir (Galvez ve Guzman, 2009) . Bilgi sistemleri, çeşitli hasarlara yol açabilecek ve büyük kayıplara neden olabilecek pek çok tehdit ile karşı karşıyadır (Peltier, 2013: 16). Literatür incelendiğinde, bilgi güvenliğini tehdit eden doğal afetler, teknik sorunlar, prosedürel eksiklikler, zararlı yazılımlar ve insan kaynaklı faktörler gibi çeşitli riskler tespit edilmiştir (Gregory, 2003: 11; Muharremoğlu, 2013: 8; Peltier, 2013: 16). Bu tehditler hem içsel hem de dışsal kaynaklardan gelebilir (Gregory, 2003: 11; Jouini, Rabai ve Aissa, 2014: 491).

İnsanlar, iyi veya kötü niyetleriyle güvenlik tehditleri oluşturabilir. Örneğin, çalışanlar yanlışlıkla dosya silebilir veya kuruluşa zarar vermek isteyen kişiler bu tehditler arasında sayılabilir (Grama, 2020: 42). Bilgi güvenliği açısından bir diğer tehdit kaynağı ise saldırganlardır (Muharremoğlu, 2013: 8). Hackerlar gibi bireyler veya gruplar, bir kuruluşun ağlarına ve sunucularına zarar vermek, bilgi çalmak veya ifşa etmek amacıyla erişim sağlamak için çeşitli yöntemler kullanabilir Bunlar arasında bilgileri çalarak internet üzerinde yayınlamak, rakiplere satmak veya kimlik hırsızlığı yapmak yer alır. Ayrıca bilgi güvenliği ihlallerini kolaylaştırmak için sosyal mühendislik gibi teknikler de kullanılır

(Gregory, 2003: 12). Doğal afetler ve kazalar gibi çevresel faktörler de bilgi güvenliğini tehdit edebilir. Bu tür tehditler genellikle öngörülemez ve kurumlar tarafından kontrol edilemez (Grama, 2020: 46). Çevresel tehditler, insan eli değmemiş faktörlerin yol açtığı zararları kapsar (Jouini ve diğer., 2014: 494). Bilgi güvenliği amaçlarına zarar verebilecek teknolojik tehditler de önemli bir kategoridir (Grama, 2020: 46; Williams, 2008: 209). Virüsler, truva atları, solucanlar ve casus yazılımlar gibi kötü amaçlı yazılımlar; donanım ve yazılım arızaları, yanlış işleyen süreçler bu tehditleri oluşturur (Grama, 2020: 46; Gregory, 2003: 12). Bu tür tehditler, bilgisayar donanımı veya yazılımına yönelik sabotaj, özel bilgilerin çalınması ve ifşa edilmesi, bilgi altyapısına yönelik saldırılar veya geniş çaplı zarara yol açmayı amaçlayan bir virüsün yayılması şeklinde gerçekleşebilir (Gregory, 2003: 11). Ayrıca fiziksel ve kimyasal süreçler de teknolojik tehdit unsurları arasında değerlendirilir (Jouini ve diğer., 2014: 494). Güvenlik açıkları, kasıtlı eylemler veya ihmal sonucunda oluşabilir (Gregory, 2003: 24). Ayrıca yapısal ve tasarımsal hatalar da güvenlik açığı olarak kabul edilir ve bu açıklar teknolojik, prosedürel veya insan kaynaklı olabilir (Grama, 2020: 45). Yazılım hataları, işlevsel sorunlardan başlayarak, saldırganların bir uygulamayı veya sistemi ele geçirmesine ve saldırmasına olanak tanıyan güvenlik açıklarına kadar geniş bir yelpazede istenmeyen sonuçlar yaratabilir (Gregory, 2003: 24).

Dinamik bilgi işleme ortamlarında sistem ve güvenlik ihtiyaçları sürekli olarak evrim geçirmektedir (Peltier, 2013: 16). Kuruluşlar, önlemlere rağmen artan maliyetlerle birlikte personel kaynaklı güvenlik ihlalleriyle karşılaşmaya devam etmektedir. Çalışanların bilgi güvenliği politikalarına ve prosedürlerine uymaması, en ciddi tehditler arasında yer almaktadır (Siponen ve diğer., 2010: 64; Diesch, Pfaff ve Krcmar, 2020: 1). Bilinçli veya bilinçsiz çalışan hataları, teknik güvenlik önlemlerinin etkisiz kalmasına yol açabilir (Özcan, 2009: 47). Kuruluşlar genellikle dış tehditlere odaklanırken, aslında kötüye kullanım olaylarının çoğu içeriden, yani çalışanlar tarafından gerçekleştirilmektedir (Chan ve diğer., 2005: 18). Bilgi güvenliği ihlallerinin ortaya çıkmasında çalışanların düşük farkındalık seviyeleri veya hiç farkındalık olmaması büyük bir etken olabilmektedir (Chan ve diğer., 2005: 19). Çalışanların bilgi güvenliği konusunda yeterince bilinçli olmaması, alınan teknolojik ve yönetimsel önlemlerin pratik etkinliğini sınırlamaktadır (Han ve diğer., 2015: 2). Sosyal mühendislik, insan etkileşimlerine dayanan ve güvenlik protokollerini ihlal etmeye yönlendiren bir yöntem olarak dikkat çeker. Bu saldırı türü, nezaket veya güven gibi insani özelliklerden yararlanarak bilgisayar sistemlerine veya korunan alanlara erişim sağlamayı amaçlar (Grama, 2020: 35).

Benzer şekilde, kurumlar tarafından işleri yürütmek üzere görevlendirilen çalışanlar, kuruma ait özel bilgileri dışarı sızdırarak güven ihlali yapabilir. Örneğin, bir çalışan ticari sırları rakip bir işletmeye satabilir, organizasyonla ilgili hassas bilgileri medyaya ifşa edebilir veya finansal bilgileri paylaşabilir (Gregory, 2003: 12). Ofiste bilgi kaynaklarının veya bilgisayar sistemlerinin kontrolsüz bırakılması, ihlallerin büyük bir kısmının dikkatsizlik sonucu meydana geldiğini göstermektedir (Chu ve So, 2020: 3).

Kurumsal kullanıcı hesabı yönetimindeki eksiklikler, kullanıcı kimliklerinin tutarsızlığı, çalışanlar ayrıldıktan sonra hesapların silinmemesi, fazla ayrıcalıklı hesaplar ve kayıt tutma süreçlerindeki yetersizlikler, etkin kullanıcı hesabı yönetimi ve incelemeleri engelleyebilir (Gregory, 2003: 24).

Kurumlar için bilgi korumanın en büyük zorluklarından biri çalışanların yetersiz bilgi, beceri ve adanmışlıktır (Thomson, Von Solms ve Louw, 2006: 7). Kurumsal bilgi güvenliği kültürünün geliştirilmesi, politika ve prosedürlerin daha iyi bir uyumla benimsenmesini sağlamalı ve böylece insan kaynaklı riskleri minimize etmelidir (Parsons ve diğer., 2015: 127). Bu bağlamda, çalışan eğitiminin önemi öne çıkmaktadır. Kurumun düzenlediği veya çalışanların katıldığı bilgi güvenliği eğitimleri, öğretim programları ve farkındalık artırıcı faaliyetler, güçlü bir kurumsal bilgi güvenliği kültürünü destekler ve çalışanların bilgi güvenliği performansını artırır (Peltier, 2013: 11). Eğitim ve farkındalık faaliyetleri, teknik olmayan önlemler içinde en kritik unsurlardandır (Colwill, 2009: 194).

1.1.2.4. Bilgi güvenliği politikaları

Bilgi güvenliği politikaları, kurumların varlıklarını koruma yöntemlerini belirten resmi dokümanlardır (Gregory, 2003: 76) ve bilgi güvenliğini yönlendiren kritik belgeler olarak işlev görür (Höne ve Eloff, 2002: 402). Bu politikalar, çalışanların kurumun güvenlik kurallarını bilmesini ve bunlara uymasını sağlamada önemli bir role sahiptir (Kim ve Han, 2019: 860). Bir kuruluşun bilgi güvenliğini koruma stratejisinde merkezi bir yere sahip olan bu politikalar, korunacak bilgi varlıklarını ve alınması gereken önlemleri açıkça tanımlar (Gregory, 2003: 76; Höne ve Eloff, 2002: 402). Bu politikalar, tüm kullanıcıların bilgi güvenliğinin önemini anlamasını sağlayacak şekilde tasarlanır ve iç tehditleri azaltmayı amaçlar (Kim ve Han, 2019: 860). Araştırmalar, bilgi güvenliği politikalarına

olan farkındalığın, güvenlik davranışlarını olumlu yönde etkilediğini göstermektedir (Li ve diğer., 2019: 19).

Literatürde bilgi güvenliği politikasının içermesi gereken bazı önemli maddeler şunlardır (Fulford ve Doherty, 2003: 113):

- Risk yönetimi ve risk analizi temelli metodolojiler kullanılmalıdır.
- Bilgi sistemleri ile ilgili yasal riskler göz önünde bulundurulmalıdır.
- Kurumun fiziksel bilgi varlıkları ve bu varlıklara erişimi koruyacak önlemler açıkça ifade edilmelidir.
- Virüs kontrol yazılımları, eklerin kullanımı ve bilgi paylaşımı politikaları net bir şekilde tanımlanmalıdır.
- Bilgilerin korunması için gerekli güvenlik seviyeleri bir sınıflandırma modeli ile belirlenmelidir.
- Güvenlik politikası, bilgi ifşaatı ve kullanımıyla ilgili tüm kısıtlamaları içermelidir.
- Kullanıcıların yetkileri ve erişim kontrolleri belirtilmelidir.
- Çalışanların sorumlulukları açıkça tanımlanmalıdır.
- Bilgilerin gizliliği, bütünlüğü ve kullanılabilirliği sağlayacak önlemler ele alınmalıdır.
- Bilgi şifreleme ve koruma gereksinimleri vurgulanmalıdır.
- Altyapı ve bilgi kaynaklarının korunmasına yönelik stratejiler ifade edilmelidir.
- Güvenlik ihlali durumunda atılacak adımlar ve bu tür olayların kaydedilmesi gereklilikleri belirtilmelidir.
- Acil durum planları, internet kullanım politikaları ve güvenli mobil bilgi işlemle ilgili uygulamalar net bir şekilde ifade edilmelidir.
- Yeni sistemlere güvenlik kontrollerinin entegrasyonu için rehberler sunulmalıdır.
- Güvenlik değerlendirmelerinin nasıl yapılacağı açıklanmalıdır.

1.2. Uzaktan Çalışma Modeli

Uzaktan ve hibrit çalışma modelleri hem işveren hem de çalışan taleplerine, ayrıca doğal sebeplerle oluşan ihtiyaçlara uyum sağlamayı amaçlayan, insan sermayesini en verimli şekilde kullanmayı hedefleyen esnek çalışma modelleridir. Bu modeller, küresel salgın öncesinde ortaya çıkmıştır ancak esnek çalışma modelleri içinde uzaktan ve hibrit

çalışmayı öne çıkaran bir süreç yaşanmıştır. Uzaktan Çalışma Modeli "İşçinin, işveren tarafından oluşturulan iş organizasyonu kapsamında iş görme edimini evinde ya da teknolojik iletişim araçları ile işyeri dışında yerine getirmesi esasına dayalı ve yazılı olarak kurulan iş ilişkisi" olarak tanımlanmaktadır (Resmî Gazete, 2016). Teknolojinin hızla gelişmesi ve dijital iletişim araçlarının genişlemesi, iş dünyasında önemli değişikliklere neden olmuştur. Bu değişimlerden biri de uzaktan çalışmadır. Uzaktan çalışma, çalışanların farklı coğrafi bölgelerde olmalarına rağmen işlerini teknoloji ve internet aracılığıyla yürütme sürecidir (Bahadır,2017:129). Uzaktan çalışma kavramı hakkında pek çok akademik çalışma yapılmış olmasına rağmen, yazında genel bir tanım üzerinde fikir birliğine varılamamıştır. Tele çalışma genelde, ana iş merkezinden ya da üretim yapılan mekândan uzakta, teknolojik cihazlar (telefon, bilgisayar veya internet erişimi olan cihazlar) kullanılarak işlerin yürütülmesi şeklinde ifade edilir (Öztürkoğlu, 2013). Uzaktan çalışmayla benzer bir konsept olan evden çalışma, özellikle teknolojik araçların kullanımını gerektirir (Soysal, 2006). Uzaktan çalışma, çalışanların ofis dışında, evlerde, kafelerde, ortak çalışma mekanlarında ya da diğer uzak yerlerde işlerini sürdürmelerine imkân tanır. Bu model hem işverenlere hem de çalışanlara çeşitli avantajlar sağlar, ancak bazı yönetimsel zorlukları da beraberinde getirir (Sokale, Alvarez ve Oluyomi, 2021). Uzaktan çalışma, işverenlere geniş bir yetenek havuzundan yararlanma fırsatı verir. Coğrafî kısıtlamaların kalkması, işverenlerin dünya genelinden en iyi yetenekleri işe almasına olanak tanır. Farklı ülkelerden uzmanların işe alınması, işe çeşitlilik ve yeni perspektifler katmakta ve böylece yenilik ve küresel işbirliğini teşvik etmektedir (Prado, Rivera ve Brookes, 2021). Ayrıca ofis maliyetlerinin düşürülmesi, işverenlerin giderlerini azaltmasına yardımcı olur. Uzaktan çalışma, çalışanların iş ve yaşam dengesini iyileştirme şansı sunar. Yoğun trafik, uzun çalışma saatleri ve ofis stresinden uzak, daha esnek bir çalışma programı oluşturabilirler. Bu durum, çalışanların daha mutlu, motive ve verimli olmalarını sağlar. Ayrıca işverenler çalışan memnuniyetini ve sadakatini artırarak, çalışan verimliliğini yükseltebilirler. Uzaktan çalışma, çevresel sürdürülebilirliği de destekler. Evden çalışma, yolculuk sürelerini ve karbon emisyonlarını azaltır, böylece enerji tüketimini düşürür ve şirketlerin fiziksel ofis alanlarını azaltmalarına veya kapatmalarına olanak tanır. Beno'nun (2021) çalışmasında, uzaktan çalışmanın çalışanların iş-yaşam dengesine olumlu katkıları ve psikolojik sağlıklarına etkileri, işveren açısından çalışan tutmanın kolaylaştırılması ve karbon ayak izinin azalması gibi sosyal ve ekonomik faydaları ortaya konmuştur.

Teknolojik gelişmeler ve dijital iletişim araçlarının geniş kullanımı, iş dünyasındaki çalışma modellerinde önemli değişikliklere yol açmıştır. Uzaktan çalışma, bu yeniliklerin en belirgin örneklerinden biridir. Uzaktan çalışma, çalışanların farklı lokasyonlarda olmalarına rağmen teknoloji yardımıyla işlerini yürütmelerini ifade eder (Bahadır, 2017: 129). Akademik literatürde bu konuda birçok çalışma olmasına rağmen, tele çalışma için standart bir tanım henüz oluşturulamamıştır. Genel olarak, tele çalışma, işin ana iş merkezinden uzak bir lokasyonda teknolojik araçlar aracılığıyla yürütülmesi olarak tanımlanabilir (Öztürkoğlu, 2013). Evden çalışma ile benzer olan bu model, teknolojik donanımların aktif kullanımını gerektirir (Soysal, 2006).

Uzaktan çalışma, çalışanların ofis dışında—evler, kafeler veya ortak çalışma alanları gibi işlerini devam ettirebilmelerini sağlar. Hem işverenlere hem de çalışanlara çeşitli faydalar sunan bu model, aynı zamanda bazı yönetimsel zorluklar getirir (Sokale, Alvarez ve Oluyomi, 2022). Uzaktan çalışma sayesinde işverenler, coğrafi sınırlamalar olmaksızın dünya genelinden yetenekleri işe alma şansına sahiptir. Bu durum işe katkı sağlayan çeşitliliği ve yenilikçi bakış açılarını artırır (Prado, Rivera ve Brookes, 2021). Ayrıca bu model sayesinde ofis giderleri azalır ve çalışanların iş-yaşam dengesi önemli ölçüde iyileşir. Uzaktan çalışma, çalışanların esnek çalışma saatlerine sahip olmalarını ve trafik gibi stres faktörlerinden uzak durmalarını sağlar. Bu durum hem çalışan memnuniyetini hem de verimliliği artırır. Çevre dostu bir model olan uzaktan çalışma, seyahat ihtiyacını azaltarak karbon salınımını düşürür ve enerji tasarrufu sağlar. Beno'nun (2021) araştırmasına göre, uzaktan çalışma iş-yaşam dengesine katkıda bulunurken, çalışanların psikolojik sağlığını iyileştirir ve işverenler için çalışan tutma kolaylığı sağlamıştır.

Uzaktan çalışmanın çeşitli modelleri vardır ve bu modeller organizasyonun yapısına, iş gereksinimlerine ve çalışanların tercihlerine göre şekillenmiştir (Pathak, Menard ve Salemi, 2022);

- Tam Zamanlı Uzaktan Çalışma: Çalışanlar ofise gitmeden tamamen uzaktan çalışırlar.
- Yarı Zamanlı Uzaktan Çalışma: Çalışanlar, belirli günlerde ofiste, diğer günlerde ise uzaktan çalışırlar.
- Esnek Uzaktan Çalışma: Çalışma saatleri ve yerleri konusunda çalışanlar ve işverenler arasında esneklik anlaşmaları yapılır.

- Proje Bazlı Uzaktan Çalışma: Çalışanlar, belirli projeler üzerinde kısa süreli uzaktan çalışırlar.
- Gezici Uzaktan Çalışma: Çalışanlar, seyahat ederken işlerini yürütmeye devam ederler.

Uzaktan çalışmanın yaygınlaşması, iş dünyasında etkili iletişim ve iş birliğinin yanı sıra, gelişmiş yönetim süreçlerini de gerektirir. Organizasyonlar ve çalışanlar, uygun teknoloji ve stratejilerle bu yeni çalışma modelinden en iyi şekilde yararlanabilir (Başol ve Cömlekçi, 2021: 755). Uzaktan çalışma, çalışanların iş-yaşam dengesini iyileştirmeye yardımcı olurken, evden çalışmanın sunduğu esneklik sayesinde aile ile geçirilen zaman artar ve bu da çalışanların genel memnuniyetini ve işteki performanslarını olumlu yönde etkilemiştir (Öner, 2017: 29).

Uzaktan çalışma, çalışanın işverenin belirlediği iş düzeni çerçevesinde evinden ya da başka mekanlardan teknoloji araçlarını kullanarak işini yerine getirmesi temeline dayalı bir iş modelidir. Resmi Gazete'de 2016 yılında yapılan tanıma göre, bu çalışma şekli yazılı bir anlaşmayla kurulan ve teknolojik iletişim araçları yardımıyla işyeri dışında gerçekleştirilen iş ilişkisini ifade eder. Bu model, çalışan ve işveren arasında gönüllülük esasına göre yürütülen ve işin nerede, ne zaman ve hangi araçlar kullanılarak yapılacağını kapsayan anlaşmaları içermektedir (ILO, 2020).

Uzaktan çalışma modeli, küresel salgından önce var olmasına rağmen, COVID-19 salgınıyla birlikte daha da ön plana çıkmış ve yaygınlaşmıştır (Tuna ve Türkmendağ, 2020). Bu süreç, esnek çalışma düzenlemelerinin gerekliliğini arttırmış ve işletmelerin insan kaynaklarını daha verimli kullanmasını sağlayarak bu modele olan ilgiyi artırmıştır. Esnek çalışma modelleri, çalışanların ve işverenlerin karşılıklı ihtiyaç ve beklentilerine uyum sağlayarak, iş ve özel hayat dengesini kolaylaştırmak amacıyla geliştirilmiştir.

Çalışma saatleri, işin yapılacağı yer, iletişim araçları ve işin denetimi gibi konular işveren ve çalışan arasında belirlenmeli ve anlaşma metnine eklenmiştir. Bu tür bir düzenleme, işlerin esnek bir şekilde yürütülmesine olanak tanırken aynı zamanda organizasyonel sınırları da genişletmiştir. Olson (1983) tarafından belirtildiği gibi, uzaktan çalışma genellikle mekan ve zaman açısından normal örgütsel sınırların ötesinde gerçekleştirmiş ve bu da çalışanlara büyük bir esneklik sunmuştur.

Günümüzde pek çok kurum, evden çalışma, uydu ofisler, ortak çalışma alanları ve mobil çalışma gibi farklı uzaktan çalışma yöntemlerini benimsemiştir (Barsness, Diekmann ve Seidel, 2005). Masaüstü ve dizüstü bilgisayarlar, cep telefonları ve ileri telekomünikasyon yazılımları, artık günlük çalışma araçları olarak kullanılmaktadır. Bu durum, uzaktan çalışmayı daha erişilebilir ve uygulanabilir hale getirmiştir (Tavares, 2017). Uzaktan çalışma modeli, salgın dönemiyle birlikte çalışma kültüründe önemli bir dönüşüm yaratmış ve işletmelerin bu yeni düzene hızla uyum sağlamalarını sağlamıştır. Bu çalışma modeli, teknolojinin sunduğu imkanlar sayesinde, işlerin zaman ve mekan sınırlarını aşarak yürütülmesine olanak tanımaktadır.

Covid-19 pandemisi, işletmelerin iş akışlarını ani bir duraklama noktasına getirerek, insanları, iş yapma şekillerinde devrim yaratan yeni bir çalışma dünyasına adım atmaya zorlamıştır. Küreselleşme etkisiyle birlikte işletmeler, rekabetçi pazar koşullarına uyum sağlamak, maliyetlerini optimize etmek, hızla evrilen teknolojik yeniliklerden faydalanmak ve inovatif çözümler sunmak zorunda kaldıklarından esnek çalışma modellerine yönelmişlerdir. Bu süreçte, işletmelerin adaptasyon kabiliyetleri kritik bir önem kazanmış, birçok iş gücü ise güvenlik önlemleri nedeniyle gece gündüz demeden uzaktan çalışma sistemine geçirilmiştir (Kniffin ve diğer., 2021). Pandemi, birçok işletmeyi, çalışanların bu yeni model için gerekli yetkinliklere sahip olmalarını sağlamadan, uzaktan çalışmayı benimsemeye büyük ölçüde mecbur bırakmıştır (Galanti ve diğer., 2021). Fiziksel ofisler, ana çalışma alanı olma özelliğini yitirmiş, uzaktan çalışma birçok kişi için 'yeni normal' haline gelmiştir. Bu durum, çalışan ve işletmeler için dijital dönüşümleri hızlandırmış ve bu hızın devamı gelecekte de büyük önem taşıyacaktır (Borg ve O'Sullivan, 2021). Şehir merkezleri neredeyse hayalet kasabalara dönüşmüş, fabrikalar, dükkanlar, oteller ve restoranlar kapatılmış, yaya trafiği ise minimum seviyelere inmişken, binlerce işletme ve çalışan, sanal ortamlarda işlerini sürdürebilmenin yollarını araştırmıştır (Banjo ve diğer., 2020). 2020 yılı boyunca, sosyal mesafeye yönelik işletme ve hükümet düzenlemeleriyle uzaktan çalışma giderek daha yaygın bir uygulama haline gelmiştir (Shimura ve diğer., 2021) ve işletmeler için bu durum, pandemi süresince bir dönüm noktası olarak değerlendirilmiştir.

Uzaktan çalışmanın yükselişi, işletmelere maliyet avantajı sağlama potansiyeli sunarken, iş gücünün büyük bir kısmının bu modele geçişi, pandemi dalgalarının tekrarlanma olasılığı göz önünde bulundurulduğunda daha da stratejik bir önem

kazanmıştır (King's College London, 2021). Uzaktan çalışma, çalışanlara ve işverenlere finansal tasarruf sağlamanın yanı sıra iş tatmini ve verimliliği artırma, daha fazla esneklik, azalan ofis masrafları, yüksek personel devamlılığı, iyileştirilmiş iş-yaşam dengesi, esnek çalışma saatleri, özerklik, işe gidip gelme süresinde azalma ve artan moral gibi çeşitli avantajlar sunmaktadır (Savić, 2020; Tavares, 2017). Ancak, uzun çalışma saatleri, yalnızlık ve iş ile ev arasındaki sınırların bulanıklaşması gibi sosyolojik ve psikolojik zorluklar da bu çalışma modelinin dezavantajları arasında yer almaktadır. Uzaktan çalışma, yüksek öz disiplin ve kişisel teknoloji araçları, iletişim ve diğer kaynaklara bağımlılık gerektirir. Ayrıca, çalışanların kurumsal bağlılık ve kültürle özdeşleşme eksikliği ile yeni çalışma yöntemleri ve eğitimlere geçiş yaparken işletmeler için ortaya çıkan ek maliyetler gibi sorunlara da neden olmuştur (Savić, 2020). Bu avantaj ve dezavantajlara rağmen, işletmeler ve çalışanlar, teknolojiye yapılan yatırımlar ve organizasyonel süreçlerin iyileştirilmesi ile uzaktan çalışmanın getirdiği değişikliklere uyum sağlayabilir (Brynjolfsson ve diğer., 2020).

1.2.1. Uzaktan çalışmanın yaygınlaşması

Uzaktan çalışma, son yıllarda iş dünyasında büyüyen bir trend haline gelmiş ve küresel çapta yaygınlaşmıştır. Bu kavram, ülkeden ülkeye farklı çalışma biçimlerine uyum sağlamakta ve doğal afetler, terör saldırıları veya pandemi gibi olağandışı durumlar sırasında iş süreçlerinin devamını sağlama konusunda kritik bir rol oynamaktadır (Tozlu, 2011). Özellikle COVID-19 pandemisi, uzaktan çalışma modellerinin benimsenmesini ve yaygınlaşmasını hızlandırmış, bu modelin iş dünyası üzerinde kalıcı değişiklikler yaratmasına neden olmuştur (Özalp, 2020: 127-132). Pandemi sürecinde, dünya genelinde alınan karantina, sosyal mesafe ve seyahat kısıtlamaları gibi önlemler nedeniyle birçok şirket ofislerini kapatarak iş süreçlerinde önemli değişiklikler yapmak zorunda kalmıştır. Bu dönemde, uzaktan çalışma, geleneksel çalışma metodlarına bir alternatif olarak hızla benimsenmiş ve geniş bir kabul görmüştür (Başol ve Çömlekçi, 2021: 756). Avrupa İstatistik Ofisi'nin yürüttüğü araştırmalar, bu eğilimin istatistiklerle de desteklendiğini göstermektedir; Avrupa Birliği'nde 2019 yılında evden çalışma oranı %5 iken, 2020 yılında bu oran %12,3'e yükselmiştir (Eurostat, 2020-2021).

Bu gelişmeler, uzaktan çalışmanın iş dünyasındaki etkilerini ve bu çalışma biçiminin modern iş pratikleri içinde nasıl bir yer edindiğini vurgulamaktadır. Uzaktan çalışma, kriz

zamanlarında iş sürekliliğini sağlamanın yanı sıra, işgücü piyasasında esneklik ve çeşitliliği teşvik etmektedir.

COVID-19 pandemisi nedeniyle birçok şirket acil olarak uzaktan çalışma sistemine geçmek zorunda kalmıştır. Bu dönemde, iş akışlarındaki düzenlemeler yapılırken, çalışanların ve genel kamu sağlığının korunması öncelikli hedefler arasında yer almıştır (Nowacki, Grabowska ve Lis, 2021). Şirketler, teknolojik altyapıların mevcudiyeti ve çevrimiçi iletişim araçlarının geniş kullanımı sayesinde bu geçiş sürecini hızlandırmıştır. Zoom, Microsoft Teams ve Slack gibi platformlar, uzaktan iş birliği ve toplantıların kolaylaşmasını sağlamıştır. Deloitte'un 2020 raporunda, dijitalleşme ve otomasyon süreçlerini entegre eden şirketlerin uzaktan çalışmaya daha sorunsuz bir geçiş yaptığı belirtilmiştir (Deloitte, 2020: 3). Pandemi, şirketlere ve çalışanlara uzaktan çalışmanın faydalarını keşfetme imkanı tanımıştır. Şirketler, bu çalışma modelinin iş sürekliliğini ve operasyonel verimliliği nasıl desteklediğini görmüşlerdir. Ayrıca işletmeler maliyet tasarrufu yaparak ofis alanlarını küçültme veya kiralama giderlerini düşürme şansı elde etmişlerdir.

Uzaktan çalışma, çalışanların iş-yaşam dengesini artırarak onlara daha esnek çalışma saatleri sunmuş ve evden çalışmanın avantajlarından yararlanmalarını sağlamıştır. Trafik ve günlük yolculuk stresinden uzak kalarak yaşam kalitesini yükseltmişlerdir (Tuna ve Türkmendağ, 2020). Çalışanlar, daha özerk bir şekilde işlerini yönetebilir ve kişisel üretkenliklerini artırabilirler. Bununla birlikte uzaktan çalışmanın pandemi sürecinde yarattığı zorluklar da göz ardı edilemez. Birçok çalışan için sosyal izolasyon, motivasyon kaybı ve iş ile özel hayat arasındaki sınırların bulanıklaşması gibi problemler yaşanmıştır (Uysal ve Yılmaz, 2020). Ayrıca evde uygun bir çalışma alanının olmaması veya dikkat dağıtıcı faktörlerin bulunması gibi zorluklar da çalışma verimliliğini etkilemiştir.

Pandemi, uzaktan çalışmayı bir zorunluluk haline getirerek iş dünyasında kalıcı bir dönüşümü tetiklemiştir. Şirketler, bu modelin sunduğu esneklik, verimlilik ve maliyet avantajlarını anlamış ve pandemi sonrası dönemde de uzaktan çalışmayı sürdürme planları yapmışlardır. Uzaktan çalışmanın, iş dünyasının geleceğinde merkezi bir role sahip olacağı ve coğrafi sınırlamalar olmaksızın işlerin yürütülebileceği bir dönem başlatması beklenmektedir. Şirketler, bu yeni çalışma biçimine uyum sağlamak ve etkili bir şekilde

yönetmek için stratejik planlamalar yapmalı ve çalışan ihtiyaçlarını karşılayacak destek sistemleri geliştirmelidir.

1.2.2. Türkiye'de uzaktan çalışma

COVID-19 salgınının Türkiye'deki ilk resmi vakası 11 Mart 2020 tarihinde tespit edilmiş, bunun ardından hükümet, virüsün yayılmasını sınırlamak amacıyla sıkı karantina tedbirleri ve sokağa çıkma yasakları getirmiştir. Pandemi döneminde, "Hayat Eve Sığar" uygulaması ile birlikte birçok sektörden işletmeler ve çalışanlar, işlerini evlerinden sürdürmeye başlamışlardır (Açıkgöz ve Mutlu, 2022).

Pandemi sürecinde, özellikle insan kaynakları, yazılım, bankacılık ve finans gibi sektörlerde uzaktan çalışma modeli yaygınlaşmış ve bu durum, şirketlerin iş yapış biçimlerinde dönüştürücü bir etki yaratmıştır (Günay ve Torgalöz, 2020: 405). Pandemi, birçok işletme için "yeni normal" olarak adlandırılan bu çalışma düzenine geçişi hızlandırmıştır (Özay, 2022). Nisan 2020'de Deloitte Türkiye tarafından yapılan bir araştırmada, pandemi öncesinde %24,2'lik bir kesimin uzaktan çalıştığı, %75,8'inin ise uzaktan çalışmadığı belirlenmiş; uzaktan çalışmanın artırılması gerektiği sorusuna %72,9 evet, %17,1 hayır ve %10 kararsız yanıtı verilmiştir. Gıda ve finans sektörleri bu yeni çalışma modeline en çabuk uyum sağlayan sektörler olarak kaydedilmiştir.

Salgının etkileriyle, uzaktan çalışma, en fazla tercih edilen yöntemlerden biri haline gelince, bu çalışma modeli için yasal düzenlemeler yapılması zorunlu hale gelmiştir. Bu gereksinime yanıt olarak, "Uzaktan Çalışma Yönetmeliği" 10 Mart 2021 tarihinde 31419 sayılı Resmî Gazetede yayımlanmıştır. Şakar ve Erkan Şahin (2021), pandemi sürecinde uzaktan çalışanların sigortalılık durumlarını inceledikleri çalışmada, Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nda uzaktan çalışmaya özgü bir düzenlemenin olmadığını belirtmişler, bu çalışanların genel sosyal sigorta kapsamında haklardan faydalanmaları gerektiğine vurgu yapmışlardır.

Pandemi sırasında yapılan değerlendirmelere göre, uzaktan çalışmanın hem olumlu hem de olumsuz sonuçları ortaya çıkmıştır. Çalışma ortamlarının fiziksel ofislerle uzak ofislerin bir karışımı olacağı görüşü yaygınlaşmış ve bu, "hibrit çalışma modeli" adı verilen yeni bir kavramın doğuşuna öncülük etmiştir (Borg ve O'Sullivan, 2021). Pandemi öncesi

çoğu işletme, ofis alanlarını çalışanların işlerini yürütebilecekleri ana mekan olarak görmekteyken, pandemiyle birlikte bu alanlar daha çok ikincil görevlerin yerine getirildiği ve rutin toplantıların yapıldığı yerler haline gelmiştir. Bilgi ve iletişim teknolojilerinin artan kapasitesi sayesinde çalışanlar, işlerinin çoğunu evden yürütebilir hale gelmiş ve bu durum, onların ev çalışma alanları ile geleneksel ofis tabanlı çalışma alanları arasında geçiş yapmalarını sağlamış, böylece hibrit çalışma modeline geçiş hızlanmıştır. Hibrit model, çalışanlara sosyal destek sağlama, bağlantıları kolaylaştırma, öğrenmeyi teşvik etme, yenilikçi iş birliğini destekleme ve yazılı olmayan ilk olarak bir kültür alanı yaratma gibi avantajlar sunmaktadır (Fayard, Weeks ve Khan, 2021).

Bu yeni çalışma düzeni, işletmelerin kiralık ofis alanlarını azaltmasına da olanak tanımıştır, böylece işletmeler hem maliyet tasarrufu sağlamakta hem de çalışanların iş-yaşam dengesini iyileştirmekte olanak bulmuşlardır.

Hibrit çalışma modeli, henüz evrensel olarak kabul görmüş bir tanımı olmasa da uzaktan çalışma yöntemlerini geleneksel ofis ortamıyla bütünleştirerek çalışma düzenlerinde bir yenilik getirmeyi amaçlamaktadır (Borg ve O'Sullivan, 2021). Bu model, çalışanların hem mekansal hem de zaman sınırlarını aşarak daha esnek ve çok yönlü bir çalışma ortamına adapte olmalarını sağlar. Hibrit çalışma, temel olarak, iş ve kişisel yaşam arasındaki sınırların belirsizleştiği, çoklu görev kabiliyetinin önem kazandığı, iş dışı kesintilerle başa çıkma gerekliliği ve sürekli öğrenme ihtiyacını kapsayan bir modeldir.

Hibrit çalışma modeli, işletmelere hem uzaktan çalışmanın avantajlarını (daha fazla esneklik, karbon ayak izinin azalması, işgücü maliyetlerinin optimizasyonu, çalışan memnuniyetinde artış) hem de geleneksel ofis ortamının sağladığı faydaları (daha etkili koordinasyon, resmi olmayan sosyal ağların oluşumu, güçlü kurumsal kültür ve yaratıcılık) sunma fırsatı vermektedir (Mortenson ve Haas, 2021). Hibrit model, işletmelerin bölümler arası ve iç süreçlerde önemli değişiklikler yapmalarını gerektiren bir yapıya sahiptir ve bu sayede geleneksel iş süreçlerinden uzaklaşarak daha yenilikçi yöntemler geliştirilmesine olanak tanır (Zeller, 2019). Hibrit çalışma düzeni, tüm çalışanların aynı düzeyde esnek çalışma becerisine sahip olmadığını, ancak iş gücünün büyük bir kısmının bu tür bir çalışma biçimiyle uyum sağlayabildiğini ortaya koymuştur (King's College London, 2021).

Ayrıca hibrit modelde bazı çalışanlar ofis ortamında, bazıları ise uzaktan çalışmayı sürdürürken, her iki grubun da teknoloji araçlarıyla desteklendiği bir iş yapısı bulunmaktadır. Modern iletişim araçları sayesinde, coğrafi olarak dağılmış takımlar işbirliği yapabilir, verimli çalışabilir ve başarılı olabilirler. Görüntülü aramalar, çevrim içi toplantılar, doküman paylaşımı ve iş birliği platformları, bu tür bir çalışma modelinde temel araçlar olarak ön plana çıkar (Workinsyn, 2020). Böylece, hibrit çalışma modelini benimsemiş kişilerin, hem yüz yüze hem de elektronik iletişim kanallarına olan güvenlerinin arttığı görülmektedir (Mayrhofer, 2021).

Hibrit çalışma modeli, çalışanların fiziksel olarak ofiste bulunmaları veya coğrafi olarak dağılmış farklı yerlerde çalışmaları gerçeğiyle işletmelerin çalışma yerlerindeki dalgalanmaları yönetme stratejilerini derinden etkilemektedir (Borg ve O'Sullivan, 2021). Bu model, örgütsel güç ilişkilerinde yeni dinamikler oluşturarak, çalışanlar arasındaki güç dengesizliklerinin işbirliğini zorlaştırabilir, örgütsel bağlılık ve genel performansı olumsuz etkileyebilir. Hibrit çalışma ortamında liderlik, yöneticilerin iki temel yetkinlik olan hibrit konumlandırma ve hibrit çalışma kapasitesini etkin bir şekilde kullanmalarını gerektirir. Bu yetkinlikler, yeni çalışma modeline uyumu kolaylaştırma ve bu modelin karşılaştığı engelleri ortadan kaldırma işlevi görür (Mortenson ve Haas, 2021).

Yöneticiler, hibrit konumlandırma süreci boyunca, çalışanların rollerini etkin bir şekilde yerine getirmeleri için gereken çalışma düzenlemeleri ve programları üzerinde anlaşmalar yapmalı, aynı zamanda çalışanların sağlığı ve esenliği üzerindeki potansiyel olumsuz etkileri azaltacak önlemleri almalıdır (ILO, 2020). Hibrit ortamlar, dinamik ve karmaşık iş koşullarına uyum sağlayabilen, esnek düşünebilen, düşük görünürlük koşullarında çalışabilen ve güvenilirliklerini ispatlayabilen çalışanları ödüllendirir. Bu durum, hibrit modelin gerektirdiği çeviklik ve uyum kabiliyetini vurgular ve bu modelde başarılı olanların, genellikle değişime hızla adapte olan ve bağımsız çalışabilme yeteneğine sahip olanlar olduğunu gösterir (Mortenson ve Haas, 2021).

Hibrit konumlandırma, çalışanların coğrafi olarak farklı yerlerde olmalarından kaynaklanan, kaynaklara erişim imkanlarında farklılıkları da beraberinde getirir. Örneğin, ofiste çalışanlar genellikle daha hızlı teknolojik altyapıya ve zengin kaynaklara hızlı erişim imkanına sahipken, uzaktan çalışanlar daha yavaş internet bağlantıları veya evden bazı kaynaklara erişememe gibi dezavantajlarla karşılaşabilirler. Bu durum, ofiste bulunan

çalışanların adaptasyon ve iş birliği süreçlerine daha rahat entegre olmalarını sağlarken, uzaktan çalışanlar için izolasyon hissi ve sosyal destek eksikliği gibi sorunlara yol açabilir (Mortenson ve Haas, 2021).

Ayrıca fiziksel olarak ayrı olan ekipler, daha fazla zamanı birebir görüşmeler yaparak veya takım toplantıları düzenleyerek geçirebilir, bu da ekip içi iletişim ve koordinasyonun artırılmasını gerektirir. Hibrit çalışma yeteneği, her bireyde eşit düzeyde bulunmayabilir; bu yetenek, etkin bir şekilde çalışabilmek için önemli bir beceri ve güç kaynağı olarak öne çıkar. Hem yüz yüze hem de sanal platformlarda güçlü ilişkiler kurabilen çalışanlar, kaynaklara kolay erişim sağlayamama gibi zorlukları aşmak için gereken kaynakları isteme, bulma ve talep etme konusunda avantajlıdır.

Hibrit çalışma modelinin dezavantajları aşağıdaki şekilde özetlenebilir;

- Çalışanların sosyalleşme fırsatlarının azalması,
- Çalışanların mesai saatleri dışında da işe yönelmeleri nedeniyle olumsuz etkilenme ihtimalleri,
- Uzaktan çalışan ekipler ile ofis içindeki ekipler arasında iletişimin zayıflaması,
- Yöneticilerin ofiste bulunan çalışanlarla daha fazla etkileşimde bulunmaları nedeniyle bu çalışanların terfi etme olasılıklarının artması ve bunun ayrıcalıklı muameleye yol açabilmesi,
- İşletme bilgilerinin saldırılara karşı korunabilmesi için güvenli bir erişim ağına ihtiyaç duyulması.

1.2.3. Uzaktan çalışmanın bilgi güvenliği üzerindeki etkileri

Uzaktan ve hibrit çalışma modellerinin ortaya çıkışı, bilgi güvenliği ortamını önemli ölçüde değiştirmiştir. Bu model, bilgi varlıklarını korumak isteyen kuruluşlar için benzersiz zorlukları da beraberinde getirmiştir çünkü geleneksel çevre tabanlı güvenlik modeli burada tam anlamı ile çalışmaz. Bu tür modellerde, güvenlik önlemleri ağırlıklı olarak bir kuruluşun fiziksel tesislerini ve dahili ağlarını korumaya odaklanır. Ancak çalışanların ev, kamusal alanlar ve ofis arasında gidip gelmesiyle güvenlik çevresi akışkan ve geniş bir hal alır. Bu değişim, erişim kontrollerinin yeniden değerlendirilmesini ve

sadece sağlam değil aynı zamanda mobil işgücüne uyum sağlayacak kadar esnek güvenlik önlemlerinin alınmasını gerektirmektedir (Figueroa, 2022).

Uzaktan çalışma modelindeki başlıca güvenlik endişelerinden biri veri ihlali riskinin artmasıdır. Çalışanlar farklı çalışma ortamları arasında hareket ederken, genellikle bazıları güvensiz veya yanlış yapılandırılmış olabilen çeşitli ağlara bağlanırlar. İşle ilgili faaliyetler için kişisel cihazların kullanılması bu riski daha da artırır. Kurumsal ekipmanın güvenlik standartlarına uymayabilen bu cihazlar, siber tehditler için potansiyel giriş noktaları haline gelir. Bu nedenle, uç noktaların güvenliğini sağlamak çok önemli hale gelmekte ve uç nokta tespit ve yanıt EDR (Endpoint Detection and Response) siber güvenlik alanında kullanılan bir teknolojidir. EDR, bilgisayarlar, mobil cihazlar ve sunucular gibi uç noktalarda gerçekleşen tehdit faaliyetlerini sürekli olarak izler, tespit eder ve yanıt verir. Sistemleri ve titiz cihaz yönetimi politikaları gibi gelişmiş çözümler gerektirmektedir. Dahası uzaktan/hibrit model verilerin güvenliğini yalnızca aktarım sırasında değil, aynı zamanda dinlenme sırasında da etkilemektedir. Çalışanlar genellikle verileri yerel olarak kişisel cihazlara kaydeder veya kolaylık sağlamak için kurumsal veri yönetimi politikalarını atlayarak yetkisiz bulut hizmetlerini kullanır. Bu tür uygulamalar veri kaybına, sızıntısına veya yetkisiz erişime yol açabilir. Bu nedenle kuruluşlar, kurumsal verilerin depolanması ve paylaşılması için kabul edilebilir uygulamaları açıkça tanımlayan veri yönetimi politikaları uygulamalıdır. Güvenli, kuruluş onaylı bulut depolama çözümlerinin kullanılmasının yanı sıra, bekleyen ve aktarılan verilerin şifrelenmesi, bu riskleri azaltmak için kritik önlemlerdir. Çalışma ortamlarındaki değişkenlik, çalışanlar arasında tutarlı güvenlik farkındalığının sürdürülmesinde de zorluklar ortaya çıkarmaktadır. Çalışanlar ev ve ofis ortamları arasında geçiş yaparken, fiziksel cihazların korunması veya kimlik avı girişimlerinin fark edilmesi gibi güvenlik uygulamaları konusunda daha az dikkatli olabilirler. Bu nedenle, sürekli bilgi güvenliği eğitimi ve farkındalık programları çok önemlidir. Bu programlar hem ofis içinde hem de dışında güvenlik uygulamalarının önemini vurgulayarak hibrit çalışma ile ilişkili belirli riskleri ele alacak şekilde uyarlanmalıdır (Esteve-Gonzalez ve diğer., 2023).

Bu zorluklara yanıt olarak kuruluşlar giderek artan bir şekilde sıfır güven güvenlik modelini benimsemektedir. Assunção (2019), ağ güvenliği için sıfır güven yaklaşımının önemini vurgulamaktadır. Ağ içindeki her şeyin güvenli olduğunu varsayan geleneksel güvenlik modellerinin aksine, sıfır güven modeli "asla güvenme, her zaman doğrula"

ilkesiyle çalışır. Bu yaklaşım, kullanıcının konumundan bağımsız olarak kaynaklara her erişim talebinin sürekli olarak doğrulanmasını gerektirdiği için özellikle hibrit çalışma ortamına uygundur. Sıfır güvenin uygulanması, çok faktörlü kimlik doğrulama ve kullanıcı davranışı, konum ve diğer bağlamsal faktörlere dayalı dinamik erişim politikaları kullanan kapsamlı kimlik ve erişim yönetimi sistemleri gerektirir. Hibrit çalışmanın bilgi güvenliği üzerindeki bir diğer önemli etkisi de BT kaynakları üzerindeki baskıdır. Dağıtık bir işgücünü destekleme ihtiyacı, BT departmanları üzerindeki taleplerin artmasına neden olabilir ve ağ bağlantısından yazılım güncellemelerine ve güvenlik yamalarına kadar daha geniş bir dizi sorunu yönetmelerini gerektirebilir. Bu durum dikkati stratejik güvenlik girişimlerinden başka yöne çekebilir. Rutin BT görevlerinin otomatikleştirilmesi ve yönetilen güvenlik hizmetlerinin kullanılması bu yükün hafifletilmesine yardımcı olarak BT personelinin daha kritik güvenlik sorunlarına odaklanmasını sağlayabilir. Ayrıca hibrit bir çalışma ortamında mevzuata uyum daha da zorlaşır. Avrupa Birliği'ndeki GDPR (General Data Protection Regulation) Genel Veri Koruma Tüzüğü gibi veri koruma yasaları kişisel verilerin işlenmesi ve gizliliği üzerinde sıkı kontroller yapılmasını zorunlu kılar (Develioğlu 2018). Verilere birden fazla, potansiyel olarak güvenli olmayan konumdan erişildiğinde uyumluluğun sağlanması, sağlam gözetim ve kontrol mekanizmaları gerektirir. Kuruluşlar, yasal gerekliliklerle uyumluluğu göstermek için veri erişimi ve işleme faaliyetlerinin kapsamlı bir denetim izini tutmalıdır (Radonić ve diğer., 2021).

Senapati ve Bharathi (2024), uzaktan çalışma ortamlarına ilişkin bilgi güvenliği tehditlerine yönelik yapılan deneysel bir çalışmada, farklı güvenlik açıklıklarını incelediler. "Uzaktan çalışma" uygulamalarına ani geçiş, deneyimli internet kullanıcıları ve yeni başlayanların siber güvenlik konularında bilgisiz olduğunu ortaya koymuştur. Çalışmada, güvenli olmayan internet alışkanlıkları, kurumsal siber güvenlik politikalarının eksikliği, güvensiz telekonferans uygulamaları ve gelişmiş siber saldırı teknikleri, uzaktan çalışma sürecinde karşılaşılan bilgi güvenliği tehditlerinin başlıca nedenleri olarak belirtilmiştir. Ayrıca, işletme yönergeleri ve güvenlik politikalarının kurumun güvenlik uyumluluğuna veya çalışanların siber güvenlik farkındalığına etkisinin bulunmadığı savunulmuştur. (Senapati ve Bharathi 2024).

İngilterede yapılan araştırmada Nottingham Üniversitesi'nden Furnell ve arkadaşları, işletmelerin ve çalışanların beklenmedik salgına ve artan siber tehditlere karşı ne kadar

hazır olduğunu araştırmıştır (Furnell ve diğer., 2020). Ofis ortamı dışında çalışma, bilgi teknolojisinin uzun zamandır vadettiği özgürlüklerden biridir. Ancak sonuçlar işletmelerin dörtte üçünde (%75) personelin evde çalışırken uyması beklenen açık siber güvenlik çerçeveli, yazılı kuralların bulunmadığını göstermiştir. Çalışanın, kuruluşun cihazlarında neler yapmasına izin verildiğini açıkça kapsayan resmi bir siber güvenlik politikasına sahip işletmelerin ise artık kullanıcı eğitimi ve farkındalığını ölçmediği için, özellikle personel eğitimini önemsemediklerine vurgu yapılmıştır. Sonuç olarak ne yazık ki, insanlarla ilgili açık bir sorun olmasına rağmen, güvenlik farkındalığı ve eğitimi genellikle "zaman kaybı" olarak görülme eğiliminde olduğu belirtilmiştir (Furnell ve diğer., 2020).

Kuruluşlardaki bilgi güvenliği uygulamalarının karmaşıklığını ve belirsizliğini anlamak ve düzenlemek için bir çerçeve sunulmalıdır. Salahuddin ve arkadaşları bilgi güvenliği uygulamalarında sıkça göz ardı edilen davranışsal unsurların incelemiştir. Şifre paylaşma, kısayol kullanma, internetten yazılım indirme gibi güvenlik prosedürlerinin ihmal edilmesi ve güvenlik kurallarının uygulanmaması gibi davranışlar, güvenlik ihlallerinin ana sebepleri olarak belirlenmiştir. Bu ihlallerin çoğunun dikkatsizlik veya politika ihlali kaynaklı olduğu analiz edilmiştir. Sonuçlar, bireylerin bilgi ve becerilerinin önemli olmasına rağmen, tek başına yeterli olmadığını göstermektedir. Olumlu bir güvenlik kültürü için çalışan davranışlarının da önemli olduğu vurgulanmıştır. Ayrıca, kişisel inançlar ve kültürün, güvenlik davranışlarını etkilediği ve davranış değişikliği için önemli olduğu belirtilmiştir. Ayrıca teknoloji, sosyal çevre, düzenleme ve kişisel çıkarların, çalışanların güvenlik davranışlarına katkı sağladığı ve bireyseli grup, organizasyonel, kültürel, modlardaki, davranışların organizasyon içinde farklı noktalarda sergilenebileceği vurgulanmıştır. (Alfawaz, Nelson, & Mohannak, 2010).

1.2.4. Uzaktan çalışmanın avantaj ve dezavantajları

Yarım yüzyıldan uzun süredir gündemde olan uzaktan çalışma, hem avantajları hem de dezavantajlarıyla sürekli tartışılan bir konu olmuştur (Bartik ve diğerleri, 2020). Bu çalışmanın bu bölümünde, uzaktan çalışma yönteminin işverenlere, çalışanlara ve topluma olan etkileri ele alınacaktır. Uzaktan çalışmanın getirdiği avantajlar ve dezavantajlar, şirketlerin ve çalışanların ihtiyaçlarına göre farklılık gösterebilir ve başarısı büyük ölçüde etkili iletişim, yönetim kabiliyeti ve teknoloji kullanımına bağlıdır.

Uzaktan Çalışmanın Avantajları

Uzaktan çalışma, viral enfeksiyonları önlemek için yaygınlaşan bir önlemdir. Çalışanlar için zaman ve para tasarrufu sağlarken, iş gücü verimliliğini artırır. Ancak, işverenler için bilgi güvenliği endişeleri doğar. Uzaktan erişim ve veri paylaşımıyla ilgili riskler artar, özellikle pandemi döneminde bu endişeler daha da artar. Ofis güvenlik araçlarının uzaktan çalışma ortamlarında uygulanamaması, bilgi sızıntısı tehdidini artırır. Bu nedenle, şirketlerin uygun güvenlik araçlarını ve politikalarını belirlemesi önemlidir.

Esneklik, uzaktan çalışmanın temel avantajlarından biri olarak kabul edilir ve çalışanlara, geleneksel ofis ortamıyla kıyaslandığında daha fazla özgürlük sunar. Çalışanlar, çalışma saatlerini ve yerlerini kendi tercihlerine göre ayarlayabilir, bu da iş ve özel hayat dengelerini iyileştirmelerine yardımcı olur (Orhan ve Karlıdağ, 2022: 404-432).

İş verimliliği açısından, uzaktan çalışmanın, ofis ortamındaki kesintilerden uzak, çalışanların işlerine daha fazla odaklanmalarını sağladığı görülmüştür; bu da işlerin daha hızlı ve verimli tamamlanmasına olanak tanır (Khudaykulov, Zheng ve Jakhongirov, 2022). Uzaktan çalışma, özellikle trafik gibi zaman kaybına ve stres yaratıcı faktörlere maruz kalmadan çalışmayı mümkün kılar. Harpaz (2002) uzaktan çalışmanın, çalışanlara nerede olurlarsa olsunlar çalışma imkanı tanıyarak iş devamsızlığını azalttığını ve motivasyonu artırdığını ifade etmiştir.

Çalışma çeşitliliği açısından, uzaktan çalışma, coğrafi sınırlamaları ortadan kaldırarak şirketlere geniş bir yetenek havuzuna erişim imkanı sunar, bu durum aynı zamanda yenilik ve küresel işbirliğini teşvik eder (Nguyen ve diğerleri, 2022). Uzaktan çalışma Ayrıca engelli bireylerin iş hayatına katılımını kolaylaştıran bir istihdam seçeneği olarak da ön plana çıkmaktadır.

Maliyet açısından, pandemi döneminde uzaktan çalışma, işverenlerin ve çalışanların maliyetlerini düşürmüştür. Ofis alanı, enerji giderleri ve diğer ofis maliyetleri azaldığı için işletmeler daha düşük maliyetle işlerini yürütebilmişlerdir (Demir, 2008: 139-145). Çalışanlar açısından bakıldığında ise, yakıt ve ulaşım maliyetleri ile yemek masraflarında azalma yaşanmıştır. Airtasker (2020) uzaktan çalışmanın bu tasarruf avantajlarına işaret ederken, bunların uzaktan çalışmanın getirdiği ekonomik faydalar arasında olduğunu

vurgulamıştır. Çalışanların her gün iş yerlerine gitmeleri, daha fazla enerji tüketimi ve buna bağlı olarak artan çevresel kirlilikle sonuçlanmaktadır (Toffler, 1983). Uzaktan çalışma modeli, çalışanların her gün ofise gitme zorunluluğunu ortadan kaldırarak enerji tüketiminde önemli düşüşlere ve dolayısıyla karbon emisyonlarının azalmasına olanak sağlamaktadır. Bu durum, çevresel sürdürülebilirlik açısından önemli avantajlar sunmaktadır (Toduk, 2023).

Uzaktan Çalışmanın Dezavantajları

Uzaktan çalışma, hem faydaları hem de zorlukları ile karmaşık bir çalışma yöntemidir. Uzaktan çalışmanın sunduğu esneklik, çalışanların işyerine gitme zorunluluğunu ortadan kaldırarak enerji tüketimi ve karbon salınımlarını azaltmış, sürdürülebilirlik adına önemli bir adım atmıştır (Toduk, 2023). Ancak bu çalışma şeklinin getirdiği iletişim zorlukları, özellikle yüz yüze etkileşimin yerini alan e-posta ve telefon gibi araçlarla daha karmaşık hale gelmiştir (Tozlu, 2011). Bu durum, anlaşmazlıkların ve iletişim hatalarının artmasına yol açabilir. İyi bir iletişim altyapısının kurulması bu sorunların üstesinden gelmede kritik önem taşır (Değirmenci, 2022).

Uzaktan çalışma, aynı zamanda çalışanların sosyal izolasyon yaşamasına ve iş yerindeki sosyal ağlardan kopmasına neden olabilir, bu da iş birliği ve koordinasyonu zorlaştırır (Orhan ve diğerleri, 2016). İş yerindeki sosyal etkileşim eksikliği, çalışanların kendilerini mesleki olarak izole hissetmelerine sebep olabilir ve bu durum, onların etkileşim ve bağlantı kurma konusunda ekstra çaba göstermelerini gerektirir (İnce ve Akbalık, 2022).

Ev ortamı, uzaktan çalışanlar için çeşitli dikkat dağıtıcı unsurlar içerebilir ve bu durum işe odaklanmayı güçleştirebilir. Çalışanların motivasyonlarını ve öz denetimlerini sürdürmeleri gerekmektedir (Gürbüzoğlu ve Ekici Gürbüzoğlu, 2019: 149-160). Uzaktan çalışma Ayrıca teknolojik altyapı ve uygun bir çalışma alanı gerektirir, bu da her çalışan için eşit olarak mümkün olmayabilir. Şirketlerin çalışanlara gerekli donanımı ve teknik desteği sağlamaları gerekirken, bu da maliyetlerin artmasına neden olabilir (Erdayı, 2012). Çalışanların kendi çalışma alanlarını oluşturmaları, tüketici fiyatlarına göre maliyetleri karşılamaları gerektirebilir (Bilginoğlu, 2021).

Uzaktan çalışma ayrıca iş ve özel yaşam arasındaki sınırların bulanıklaşmasına neden olabilir. Evde çalışmak, çalışanların kişisel ve iş yaşamları arasında net bir ayrım yapmalarını zorlaştırabilir. Özellikle kadın çalışanlar, kişisel yaşam rolleri ile iş yükünün artması arasında denge kurmakta zorlanabilirler. Pandemi süresince evde tüm bireylerin bulunması, kadınların ev işleri ve bakım sorumlulukları üzerindeki baskıyı artırırken, iş performansları üzerinde ek stres yaratmıştır (Zeybekoğlu ve Dursun, 2020; Kıcır, 2019). Bu durumlar, uzaktan çalışmanın avantajları kadar dezavantajlarını da gözler önüne sermektedir.

1.2.5. Uzaktan çalışmanın örgüt üzerindeki etkileri

Uzaktan çalışma, günümüz iş dünyasında giderek daha fazla benimsenen bir model haline gelmiştir ve bu model, organizasyonlarda önemli bir dönüşüm sürecini başlatmaktadır. Uzaktan çalışma, çalışanlara iş ve özel yaşamlarını daha iyi dengeleme olanağı sunarak, motivasyon ve memnuniyetlerini artırma avantajına sahiptir (Arregi, Gago ve Legarra, 2022). Ancak yüz yüze etkileşimin eksikliği, uzaktan çalışmanın en büyük dezavantajlarından biri olarak karşımıza çıkmaktadır. Hertel (2005) ve Ammons (2004) çalışmalarında, elektronik iletişim araçlarının yüz yüze iletişimin yerini almasının, sosyal ve profesyonel roller üzerinde etkili olduğunu ve iletişim problemlerine yol açabildiğini belirtmişlerdir. Uzaktan çalışanlar, iş yerindeki fiziksel ofis ortamından uzak kaldıklarında, meslektaşlarıyla olan etkileşimlerinde zorluklar yaşayabilirler (Banita, 2009). Uzaktan çalışmanın tetiklediği izolasyon, profesyonel ve sosyal olmak üzere iki ana grupta incelenebilir (Kurland ve Cooper, 2002). Profesyonel izolasyon, çalışanların örgüt içindeki meslektaşlarıyla kişilerarası ağ kurma ve informal öğrenme fırsatlarından mahrum kalmalarını içerirken, sosyal izolasyon, çalışanların iş yaşantısındaki sosyal ve profesyonel ağlardan uzaklaşmalarını ifade eder. Uzaktan çalışma, aynı zamanda etkili iletişim sağlama zorunluluğunu da beraberinde getirir. Elektronik iletişim araçları, yüz yüze iletişimde bulunan ses tonu, mimikler ve beden dili gibi önemli unsurları barındırmadığı için, iş süreçlerindeki iletişim eksikliği öne çıkar (Bhat ve diğerleri, 2016). Uluslararası Çalışma Örgütü (2020), bilgi akışının sürekliliğinin ve kalitesinin korunması gerektiğini vurgularken, Lipnack ve Stamps (2010), çalışan ekipler arasında yüksek kaliteli iletişimin sağlanması için projelerin yüz yüze veya video konferans yoluyla başlatılmasını önermektedir. Ayrıca iş süreçleri ve çıktıların belgelenmesi, her çalışanın bu bilgilere erişebilir olması gerektiğine dikkat çekmektedirler. Sonuç olarak, uzaktan çalışma modeli,

çalışma hayatında esneklik ve denge sunmasının yanı sıra, iletişim zorlukları ve sosyal izolasyon gibi dezavantajlar da getirmektedir. Bu dezavantajların üstesinden gelmek için, organizasyonların etkili iletişim stratejileri geliştirmeleri ve çalışanların sosyal bağlarını güçlendirmeleri önem taşımaktadır.

Bağlılık Örgütsel bağlılık, çalışanların bir örgüte duyduğu bağlılığı ve bu örgütte kariyerlerini sürdürme isteklerini açıklayan psikolojik bir kavramdır (O'Reilly ve Chatman, 1986). Çalışanların örgütsel bağlılığı, bireysel amaçlarının örgütün vizyonuyla uyum sağlaması halinde güçlenir ve bu da onların örgütte kalma kararlarını etkiler (Ghani ve diğer., 2004). Uzaktan çalışma, esneklik sağlaması ve iş-yaşam dengesine katkıda bulunmasıyla çalışanların örgütsel bağlılığını artırır, ayrıca işten ayrılma oranlarını azaltarak işverenlerin yetenekli çalışanları elde tutmasına yardımcı olur (Ayyıldız, Çam ve Kuş, 2021: 136-149). Bununla birlikte uzaktan çalışma, sosyal izolasyon gibi olumsuz etkileri de beraberinde getirir, bu da çalışanların örgütsel etkileşime katılımını zorlaştırabilir (Cai ve diğerleri, 2019).

Allen ve Meyer (1990), örgütsel bağlılığı üç farklı bileşene ayırır:

Duygusal bağlılık: Çalışanın örgüte duygusal olarak bağlı olması ve burada bulunmaktan memnuniyet duymasıdır.

Devam bağlılığı: Çalışanın yatırım yapmış olduğu zaman ve çabanın karşılığında örgütten ayrılmanın maliyetini ve kayıplarını değerlendirerek örgütte kalmaya karar vermesidir.

Normatif bağlılık: Çalışanın örgütte kalmanın bir yükümlülük olduğunu hissetmesi ve ahlaki bir zorunluluk olarak örgütte devam etmesidir.

Taborosi ve diğerleri (2020) tarafından yapılan bir araştırma, uzaktan çalışanların, geleneksel çalışma ortamındaki meslektaşlarına kıyasla, uygun koşullar sağlandığında örgütsel özdeşleşme, takım üyelerine ve yöneticilere olan güveni artırarak daha güçlü bir örgütsel bağlılık gösterdiğini ortaya koymuştur. Bu koşullar; takım üyelerine ve yöneticilere duyulan güven ile örgütsel özdeşleşmenin sağlanmasıdır. Ayrıca Ajuha ve diğerleri (2002) tarafından yapılan çalışma, hem geleneksel hem de sanal/uzaktan çalışma

düzeninde, iş tatmini ve örgütsel bağlılığın çalışanların işten ayrılma niyetini etkileyen önemli faktörler olduğunu belirtmiştir. Bu, örgütsel bağlılığın, çalışma biçiminden bağımsız olarak işten ayrılma niyetinin bir belirleyicisi olduğunu göstermektedir. Bu bağlamda, uzaktan çalışma sürecinde örgütsel bağlılığın ve etkileşimin desteklenmesi, çalışanların işten ayrılma oranlarını düşürmek ve genel memnuniyetlerini artırmak için hayati önem taşır.

İş Tatmini ve motivasyon

Çalışanların iş tatmini ve motivasyon seviyeleri, onların performansını doğrudan etkileyip işletmelerin genel hedeflerine ulaşmalarına katkı sağlar (Başol ve Çömlekçi, 2021: 755-776). İş tatmini ve motivasyonun yüksek olması, çalışanların işlerini daha verimli yapmalarını sağlar ve bu durum da işletmelerin başarısını destekler.

İşletmeler, çalışanların iş tatmini ve motivasyonunu ölçmek ve artırmak için çeşitli araçlar kullanabilir. Anketler, geri bildirim oturumları ve düzenli performans değerlendirmeleri, çalışan memnuniyetini ve ihtiyaçlarını anlamada önemli yöntemlerdir (Sokale, Alvarez ve Oluyomi, 2022). Bu bilgiler, işletmelerin çalışanlarına yönelik iyileştirme ve destek stratejileri geliştirmelerine olanak tanır.

İş tatmini ve motivasyonu artırmak amacıyla, işletmelerin geri bildirim sağlama, eğitim ve kariyer gelişim fırsatları sunma, adil ödüllendirme sistemleri kurma ve çalışanların takım içinde işbirliği yapmalarını teşvik etme gibi çeşitli stratejileri hayata geçirmeleri önerilir. Bu tür stratejiler, çalışanların iş yerindeki memnuniyetini ve motivasyonunu artırarak, onların daha bağlı ve üretken olmalarına yardımcı olur (Keser ve Bilir, 2019).

Sonuç olarak, iş tatmini ve motivasyon, çalışan performansını ve dolayısıyla işletmenin genel başarısını belirleyen kritik faktörlerdir. İşletmelerin, çalışanlarının tatmini ve motivasyonunu sürekli olarak değerlendirip bu yönde stratejiler geliştirmesi, sürdürülebilir bir rekabet avantajı yaratmalarını sağlar.

Liderlik ve yönetim

Liderler, örgütler içinde çalışanları ortak hedefler doğrultusunda yönlendirerek motivasyon ve teşvik gibi ihtiyaçları karşılayan, etki gücünü stratejik bir şekilde kullanan kişilerdir (Tağraf ve Çalman, 2009:137; Seyfikli, 2007). Uzaktan çalışma, liderlik için önemli bir dönüşüm süreci sunmaktadır çünkü teknolojik gelişmelerle birlikte iş yerlerinin dinamikleri değişmektedir. Bu gelişmeler, ofislerin fiziksel sınırlarını aşarak iş süreçlerini sanal ortamlara taşımış, zaman ve mekan bağımsızlığını getirmiştir (Kayra, 2022:289). Geleneksel yüz yüze çalışma yöntemlerinde liderler genellikle kontrol odaklı bir yaklaşım sergilerken, sanal çalışma ortamlarında ise liderlerin esneklik ve düzenleme yapma yeteneği ön plana çıkmaktadır (Özdemir ve Erkutlu, 2017).

Sanal çalışma ortamına geçiş sürecinde liderlerin bu yeni duruma uyum sağlamaları gerekmektedir. Taş ve diğerleri (2020) sanal ortamda liderliğin boyutlarını şöyle açıklamışlardır:

Sanal Teknoloji Yeterliği: Liderlerin, örgüt için uygun yazılım ve bilişim teknolojilerini seçme, kullanma ve değerlendirme konusunda yetkin olmaları gerekmektedir. Bu, sanal iletişim araçlarını etkin ve güvenli bir şekilde kullanabilme, örgüt kültürünü sanal ortamda sürdürebilme ve elektronik öğrenmeyi entegre edebilme kabiliyetini içerir. Ayrıca bu süreçte etik ilkeleri gözeterek güven inşa etmek de liderin sorumlulukları arasındadır.

Sanal İletişim Yeterliği: Liderlerin sanal ortamlarda da güçlü iletişim becerilerini sürdürmeleri, iletişim engellerine rağmen hedef odaklılığı korumaları ve örgüt içi iletişimin sürekliliğini sağlamaları önemlidir.

Sanal Ekip Yönetimi Yeterliği: Liderler, sanal ortamlarda da örgütsel ve bireysel hedefleri destekleyecek şekilde ekiplerin becerilerini geliştirmeli, etkileşimi kolaylaştıracak sanal ekipler kurmalı ve bu ekipleri iş süreçlerinde doğru yönlendirerek performanslarını izlemelidir.

Bu yeterlilikler, uzaktan çalışma modellerinde liderlerin karşılaşabileceği zorluklara uyum sağlamalarını ve ekiplerini başarıyla yönetmelerini destekleyecektir. Örgütlerin

liderlik yapısını bu yeni çalışma şekline adapte etmeleri hem iş süreçlerinin verimliliğini hem de çalışanların bağlılığını ve memnuniyetini artırma potansiyeline sahiptir.

Liderler, örgütlerde çalışanları birleşik hedeflere yönlendirerek motivasyon ve teşvik ihtiyaçlarını karşılarlar. Özellikle uzaktan çalışma düzeninde, liderlerin bu rolleri daha karmaşık hale gelmektedir. Uzaktan çalışma, fiziksel ofis ihtiyacını ortadan kaldırmış, iş düzenlemelerini zaman ve mekân bağımsızlığına kavuşturmuştur (Kayra, 2022:289). Geleneksel ofis ortamında liderlik daha çok kontrol odaklıyken, sanal çalışma ortamlarında liderler, çalışanlara daha fazla esneklik ve düzenleme yetkisi sağlamalıdır (Özdemir ve Erkutlu, 2017).

Uzaktan çalışma ortamında liderler için iletişim, esas becerilerden biridir. Liderlerin açık, net ve düzenli iletişim kurmaları, beklentileri paylaşmaları, geri bildirim sağlamaları ve çalışanların sorularını yanıtlamaları gerekmektedir. Ayrıca sanal toplantılar ve video konferanslar gibi iletişim araçlarının etkin kullanımı önemlidir (Sokale, Alvarez ve Oluyomi, 2022). Uzaktan çalışma sırasında liderler, çalışanlara işlerini etkili bir şekilde yönetme ve sorumluluk alma özgürlüğü vererek, çalışanların ihtiyaçlarına duyarlı ve destekleyici olmalıdır.

Liderlerin kişisel rol yeterliliği, örgütün vizyon ve hedeflerine uygun olarak projeleri organize etme, süreçlerde performansı değerlendirme ve karar verme süreçlerinde sanal ekipleri dahil etme yeteneğini içermelidir. Bu, örgüt içinde çatışmaları yönetme ve astların gelişimine destek olma yeteneğini de kapsar (Tağraf ve Çalman, 2009:137; Seyfikli, 2007).

Uzaktan çalışma, sanal ekip yönetimi becerilerini gerektirir. Liderlerin, örgütsel ve bireysel hedeflere hizmet etmek için çalışanların yeteneklerini geliştirmeleri, sanal ekipleri etkin bir şekilde yönetmeleri ve bu ekiplerin performansını sürekli izlemeleri gerekir. Bu, çalışanların izolasyondan uzak, motive edici ve katılımcı bir çalışma ortamı yaratılmasını sağlar.

Sonuç olarak, uzaktan çalışma, işletmelere ve çalışanlara çeşitli avantajlar sunarken, liderlik ve yönetim süreçlerinde önemli değişiklikleri de beraberinde getirir. İşletmeler, başarılı bir uzaktan çalışma modeli yürütmek için etkili politikalar ve iletişim stratejileri

geliştirmeli, çalışanların yaratıcılığını ve işbirliğini teşvik eden ortamlar oluşturmalıdır (Bahadır, 2017: 129-134).

Başol ve Çömlekçi (2021) uzaktan çalışma yönetiminin, geleneksel iş yönetimi pratiklerinden ayrı olarak özel stratejiler gerektirdiğine işaret etmişlerdir. Uzaktan çalışmanın başarılı bir şekilde yönetilmesi, açık ve etkin uzaktan çalışma politikalarının belirlenmesine bağlıdır. Bu politikalar; uygun pozisyonlar, çalışma saatleri, performans ölçütleri, iletişim ve raporlama tekniklerini kapsamalı ve şirketler bu politikaları çalışanlara net bir şekilde açıklamalıdır (Wickramasinghe ve Nakandala, 2022: 153-176). Son olarak, Taştan (2022) uzaktan çalışma politikalarının, örgüt kültürüne uyum sağlaması ve bu kültürün devamlılığını garantilemesi gerektiğini belirtmiştir. Bu bağlamda, çalışanların düzenli aralıklarla ofiste fiziksel olarak bir araya gelmeleri, eğitim programları ve performans değerlendirme toplantıları düzenlenmesi önerilmektedir. Bu stratejiler, uzaktan çalışma düzeninde bile örgüt kültürünün sürdürülebilirliğini sağlamak için kritik öneme sahiptir.

1.3. Bilgi Güvenliği ve Uzaktan Çalışma İlişkisi

Modern işyerinde uzaktan çalışmanın yaygınlaşması, bilgi güvenliği uygulamalarının derinlemesine yeniden değerlendirilmesini gerektirmiştir. Bu değişim büyük ölçüde geleneksel işyeri ortamının dağılmasından kaynaklanmaktadır; çalışanlar artık merkezde değil, çeşitli yerlere dağılmış durumdadır ve potansiyel olarak güvensiz ağlar üzerinden kurumsal kaynaklara erişmektedir. Bilgi güvenliği ve uzaktan çalışma arasındaki ilişki bu nedenle yeni zorluklarla karakterize edilmekte ve hassas veri ve sistemleri korumak için yenilikçi stratejiler gerektirmektedir. Uzaktan çalışma ortamlarındaki temel endişelerden biri, veri ihlali riskinin artmasıdır. Uzak konumlardan çalışanlar genellikle kişisel veya daha az güvenli internet bağlantılarına güvenirler ve bu da kötü niyetli aktörler tarafından ele geçirilmeye açık olabilir. Buna ek olarak, kurumsal ekipman kadar titizlikle korunmayan kişisel cihazların kullanımı daha fazla güvenlik açığı ortaya çıkarır. Bu cihazlar en son güvenlik güncellemelerinden yoksun olabilir veya birden fazla aile üyesi tarafından kullanılıyor olabilir, bu da kazara maruz kalma veya kötü amaçlı yazılım bulaşma riskini artırır. Bu güvenlik açıklarını gidermek için kuruluşlar, uzaktan çalışma bağlamına özel olarak uyarlanmış sağlam siber güvenlik politikaları uygulamalıdır. Bu, aktarım sırasında verileri şifreleyen sanal özel ağların (VPN'ler) kullanımını içerir ve

hassas bilgilerin halka açık veya güvenli olmayan ağlar üzerinden iletildiğinde bile gizli kalmasını sağlar. Ayrıca çok faktörlü kimlik doğrulamanın (MFA) kullanılması, kurumsal kaynaklara erişim izni vermeden önce kullanıcıların kimliğini birden fazla kimlik bilgisi aracılığıyla doğrulayarak ek bir güvenlik katmanı sağlar (Şakar ve Şahin, 2021).

Uzaktan çalışma ve bilgi güvenliği bağlantısının bir diğer önemli yönü de sürekli izleme ve müdahale yeteneklerine duyulan ihtiyaçtır. Uzaktan çalışan işgücünün dağıtık yapısı, BT departmanlarının tüm erişim noktaları ve cihazlar üzerindeki görünürlüğünü engelleyerek güvenlik olaylarını tespit etmeyi ve bunlara anında müdahale etmeyi daha zor hale getirebilir. Bu nedenle kuruluşlar uç nokta koruması, veri kaybı önleme ve anormallik tespiti özellikleri sunan gelişmiş güvenlik araçlarına yatırım yapmalıdır. Bu araçlar, bir güvenlik ihlaline işaret edebilecek olağandışı faaliyetlerin belirlenmesine yardımcı olarak zamanında müdahale edilmesini sağlayabilir. Ayrıca uzaktan çalışma düzeninde veri yönetişimi kritik bir önem kazanır. Kuruluşlar, içeriden gelen tehditler ve kazara verilere maruz kalma riskini en aza indirmek için rollere ve sorumluluklara dayalı olarak veri erişim haklarını ve ayrıcalıklarını açıkça tanımlamalıdır. Veri depolama ve aktarımına ilişkin politikalar da titizlikle uygulanmalı ve hassas bilgilerin hem bekleme hem de aktarım sırasında depolanması için şifreleme zorunlu bir uygulama olmalıdır (Malecki, 2020).

1.4. Bilgi Güvenliği Eğitimi ve Farkındalığı

İnsan faktörü, herhangi bir kuruluşun güvenlik duruşunda çok önemli bir rol oynar. Bilgi güvenliği eğitimi ve farkındalık programları, çalışanların potansiyel güvenlik tehditlerini tanımaları ve azaltmaları için gerekli bilgi ve becerilerle donatılmasında temel araçlardır. Bu programlar yalnızca düzenleyici bir gereklilik değil, proaktif bir güvenlik stratejisinin temel bir bileşenidir. Bilgi güvenliği eğitimi ve farkındalık girişimleri, kurumun özel ihtiyaçlarının kapsamlı bir değerlendirmesiyle başlamalıdır. Bu, işin doğasına ve operasyonel bağlamına dayalı olarak en ilgili tehditlerin belirlenmesini içerir. Eğitim içeriği bu spesifik tehditleri ele alacak şekilde uyarlanmalı ve rolleri ne olursa olsun tüm çalışanların kurumun dijital varlıklarını korumadaki rollerini anlamaları sağlanmalıdır. Etkili bir eğitim programı aynı zamanda ilgi çekici ve erişilebilir olmalıdır. Bu, interaktif modüller, atölye çalışmaları ve haber bültenleri veya intranet gönderileri yoluyla düzenli güncellemeler gibi çeşitli formatlarla sağlanabilir. Öğrenme süreçlerinin oyunlaştırılması,

sınavlar ve ödüller gibi unsurların dahil edilmesi, katılımı ve bilgilerin akılda tutulmasını artırabilir. Ayrıca bu programlar tek seferlik bir etkinlik değil, yeni ve gelişen güvenlik sorunlarını ele almak için düzenli güncellemelerle sürekli bir süreç olmalıdır (Alshaikh ve diğer., 2018).

Farkındalık kampanyaları da aynı derecede önemlidir ve kurum içinde güvenlik bilincine sahip bir kültür yaratmaya odaklanmalıdır. Bu kampanyalar, güvenlik ihlallerinin gerçek dünyadaki sonuçlarını göstermek için hem kurum içi hem de kurum dışı son güvenlik olaylarını vurgulayabilir. Ayrıca çalışanlara güçlü şifrelerin önemi, kimlik avı saldırılarıyla ilişkili riskler ve hassas bilgilerin uygun şekilde kullanılması gibi en iyi uygulamaları hatırlatmaya da hizmet ederler. Dahası bilgi güvenliği farkındalığı resmi eğitim oturumlarının ötesine geçmeli ve kurumun faaliyetlerinin her yönüne nüfuz etmelidir. Üst yönetim, bilgi varlıklarını koruma taahhüdünü göstererek bir güvenlik kültürünü aktif bir şekilde teşvik etmelidir. Bu yukarıdan aşağıya yaklaşım, kurumun tüm seviyelerinde güvenliğin öneminin pekiştirilmesine yardımcı olur (Mcllwraith, 2021).

1.5. Bilgi Güvenliği Politikalarının Rolü

Bilgi güvenliği politikaları, bir kuruluşun bilgi varlıklarını yönetme ve koruma yaklaşımına rehberlik eden temel belgelerdir. Bu politikalar beklentileri belirlemek, rolleri ve sorumlulukları tanımlamak ve veri ve ağ güvenliği için bir yönetişim modeli oluşturmak için bir çerçeve sağlar. Bilgi güvenliği politikalarının rolü, elektronik ve fiziksel bilgi kaynaklarının güvenliğini yöneten standartların ve prosedürlerin ifade edilmesinde çok önemlidir. Bu politikaların geliştirilmesi ve uygulanması yapılandırılmış bir yaklaşım gerektirir. İlk olarak, bilgi varlıklarının tanımlanmasını ve sınıflandırılmasını, hassasiyetlerinin ve maruz kalmaları veya kaybolmaları ile ilgili potansiyel risklerin değerlendirilmesini içerir. Bu değerlendirme, uygulanması gereken uygun güvenlik kontrolleri ve önlemleri seviyesinin belirlenmesine yardımcı olur. Bilgi güvenliği politikaları ayrıca kuruluşun genel stratejik hedeflerinin yanı sıra hükümetler ve endüstri standartları tarafından belirlenen uyumluluk gerekliliklerleriyle de uyumlu olmalıdır. Bilgi güvenliği politikaları geliştirildikten sonra kuruluş genelinde güvenlik önlemlerinin uygulanması için bir plan görevi görür. Kullanıcı izinlerinin yönetimi, şifreleme uygulamaları ve olay müdahale stratejilerini içeren hassas bilgilerin işlenmesi ve korunmasına yönelik protokolleri belirlerler. Bu protokolleri net bir şekilde ortaya koyan

politikalar, kuruluş genelinde tutarlı olan standart bir güvenlik yaklaşımı olmasını sağlar. Bu tekdüzelik, bilgilerin bütünlüğünü ve gizliliğini korumak için çok önemlidir (Nwankpa ve Datta, 2023).

Güvenlik uygulamaları için bir dizi direktif sağlamanın yanı sıra, bilgi güvenliği politikaları bir kuruluş içindeki güvenlik kültürünü şekillendirmede de kritik bir rol oynar. Çalışanlar için bir eğitim aracı olarak hizmet ederler ve güvenliği sağlama konusundaki sorumluluklarını anlamalarına yardımcı olurlar. Bu politikalara dayalı düzenli eğitim oturumları, personel arasında farkındalığı ve uyanıklığı artırabilir, bu da güvenlik ihlallerini önlemede çok önemlidir. Yönergeler hakkında bilgi sahibi olan çalışanların bunlara uyma ve bir güvenlik tehdidinden şüphelendiklerinde uygun şekilde yanıt verme olasılıkları daha yüksektir. Ayrıca bilgi güvenliği politikaları hesap verebilirliğin tesis edilmesinde önemli bir rol oynar. İhlalin ciddiyetine bağlı olarak disiplin cezalarını veya yasal sonuçları içerebilecek uyumsuzluk sonuçlarını tanımlarlar. Bu düzeyde bir hesap verebilirlik sadece caydırıcılık açısından değil, aynı zamanda çalışanlar arasında sorumluluk duygusunun geliştirilmesi açısından da önemlidir. Politikalar, denetim ve izleme faaliyetleri için bir temel sağlayarak güvenlik ekiplerinin belirlenen standartlara uyumu değerlendirmesine ve gerekirse düzeltici önlemler almasına olanak tanır. Bilgi güvenliği tehditlerinin dinamik yapısı, politikaların düzenli olarak gözden geçirilmesini ve güncellenmesini gerektirir. Teknolojik gelişmeler, ortaya çıkan tehditler ve düzenleyici gerekliliklerdeki değişiklikler mevcut politikaları hızla geçersiz kılabilir. Bu nedenle, periyodik gözden geçirme ve revizyon için politikalara bir mekanizma dahil edilmelidir. Bu süreç, politikaların yeni güvenlik sorunlarını ele almada güncel ve etkili kalmasını sağlar. Dahası bilgi güvenliği politikaları bir kurumun iç operasyonlarının ötesine uzanır. Bunlar aynı zamanda verilerin, kuruluşun kendisiyle aynı standartlara uyması gereken satıcılar ve iş ortakları gibi üçüncü taraflarca nasıl ele alınacağını da yönetir. Bu, bilginin sınırlar ötesinde ve kurumlar arasında aktığı dijital bir ekosistemde özellikle önemlidir. Kuruluşlar sıkı güvenlik politikaları uygulayarak üçüncü taraf kanallar aracılığıyla meydana gelebilecek veri ihlalleri riskini azaltabilirler (Safa ve diğer., 2016).

2. ARAŞTIRMA

2.1. Araştırmanın Amacı ve Önemi

Bilgi altyapısının korunması, araştırmacılar ve uygulayıcılar için önemli bir zorluktur. Bu nedenle uyumu artırmak için mevcut bilgi birikiminin zenginleştirilmesi gerekmektedir. Ancak, Türkiye'de uzaktan veya hibrit çalışanların bilgi güvenliği davranışlarını araştıran bir çalışmaya literatürde rastlanmamıştır.

Bu nedenle araştırmada, uzaktan veya hibrit çalışma modelini benimseyen işletmelerde çalışanların, bilgi güvenliğine yönelik davranışları hakkında bilgi edinmek amacıyla ölçek uyarlaması yapmak hedeflenmiştir. Elde edilen istatistiksel sonuçlar, bireylerin bilgi güvenliği davranışlarını şekillendirmesinde ve işletmelerin bilgi güvenliği politikalarına ışık tutması amacıyla kullanılacaktır. Bu kapsamda çalışanların bilgi güvenliği davranışı ölçeği ifadelerinden oluşan anket formu Google Forms üzerinden elektronik anket formu şeklinde oluşturularak, Türkiye'de Ankara ilinde yaşayan, farklı sektörlerde uzaktan veya hibrit çalışan, 320 katılımcıya uygulanmıştır.

2.2. Araştırma Yöntemi ve Soruları

Çalışmada Saeed tarafından 2023 yılında geliştirilen Dijital Çalışma Ortamları ve İşletme Çalışanlarının Bilgi Güvenliği Davranışları ölçeği Türkçeye uyarlanmıştır (Saeed 2023). Ankette, "Kesinlikle Katılıyorum"dan "Kesinlikle Katılmıyorum'a" kadar uzanan 5'li Likert tipi ölçek kullanılmıştır. Bu sayede, katılımcıların görüşleri kapsamlı bir şekilde değerlendirilebilmektedir. Ayrıca, konu hakkında bilgisiz veya tarafsız olanlar için "Ne katılıyorum ne de katılmıyorum" gibi bir orta seçenek de bulunmaktadır.

2.3. Araştırmanın Evreni ve Örneklem

Araştırmanın evrenini Ankara ilinde yaşayan ve uzaktan veya hibrit çalışma modelinde çalışan bireyler oluşturmaktadır. Bu kriterleri sağlayan farklı sektörlerde çalışan

bireylerle anket linki paylaşılmış ve böylece anketin farklı çevrelere yayılması sağlanmıştır.

Araştırmanın saha uygulaması 20 Kasım 2023 tarihinde başlatıp, 5 Mayıs 2024 tarihinde sonlandırılmıştır. Araştırmaya 320 kişi katılmıştır.

2.4. Araştırma Sınırlılıkları

Araştırma kapsamında anket çalışmasının dijital yöntemle gerçekleştirilmesinin, yüz yüze görüşme ile elde edilebilecek verilere ulaşılamaması ve uzaktan çalışan insanlara ulaşmanın zorluğu çalışmanın kısıtını oluşturmaktadır.

2.5. Araştırma Verilerinin Değerlendirilmesi

Çalışmada Saeed tarafından 2023 yılında geliştirilen Dijital Çalışma Ortamları ve İşletme Çalışanlarının Bilgi Güvenliği Davranışları Türkçeye uyarlanarak kullanılmıştır. Anket soruları EK-1'de yer almaktadır.

Araştırmada uygulanan anket formu 7 bölümden oluşmaktadır. Birinci bölümde katılımcıların kişisel bilgilerini ve demografik verilerini içeren sorular sorulmuştur. Bu bölümde çalışma şekli, cinsiyet, yaş grubu, eğitim seviyesi ve çalışma alanı ile ilgili sorular yer almaktadır. İkinci bölümde, katılımcıların bilgisayar ve şifre yönetimi alışkanlıklarına yönelik sorular bulunmaktadır. Bu bölümde şifre kullanımı ve yönetimiyle ilgili sorular sorulmuştur. Üçüncü bölümde, katılımcılara güvenlik yazılımları ve uygulamaları ile ilgili sorular yöneltilmiştir. Bu bölümde antivirüs programları, güvenlik duvarı ve casus yazılım önleme araçları ile ilgili sorular yer almaktadır. Dördüncü bölümde, katılımcılara e-posta güvenliği ile ilgili sorular sorulmuştur. Bu bölümde e-posta kullanımı ve şifreleme ile ilgili sorular bulunmaktadır. Beşinci bölümde, katılımcılara şirket politikaları ve güvenlik farkındalığı ile ilgili sorular yöneltilmiştir. Bu bölümde şirketin güvenlik politikalarına uyum ve farkındalık ile ilgili sorular yer almaktadır. Altıncı bölümde, katılımcılara eğitim ve farkındalık ile ilgili sorular sorulmuştur. Bu bölümde bilgi güvenliği eğitimi ve güvenlik farkındalığı ile ilgili sorular bulunmaktadır. Yedinci bölümde ise, katılımcılara güvenlik algıları ile ilgili sorular sorulmuştur. Bu bölümde bilgisayar güvenliği algısı ve endişe düzeyi ile ilgili sorular yer almaktadır.

Her bölüm, kullanıcıların farklı yönlerden bilgi güvenliği konusundaki davranışlarını ve tutumlarını ölçmek için tasarlanmıştır.

Anket formunda, birinci bölümde 5 soru, ikinci bölümde ise 6 soru, üçüncü bölümde 8 soru, dördüncü bölümde 4 soru, beşinci bölümde 5 soru, altıncı bölüm: 3 soru, yedinci bölüm: 6 soru olmak üzere toplam 37 sorudan oluşmaktadır. İlk 5 soru katılımcıların, yaş, sektör gibi sosyo-demografik özelliklerine yönelik sorulardan oluşmakta olup çoktan seçmeli ve açık uçlu sorulardan oluşmaktadır. Sonraki 32 soru ise katılımcıların elektronik sağlık kayıtları hakkında farkındalık ve beklentilerini ölçmeye yönelik 5'li Likert (1: Kesinlikle Katılıyorum, 2: Katılıyorum 3: Kararsızım, 4: Katılmıyorum, 5: Kesinlikle Katılmıyorum) ile ölçeklendirilmiştir.

3. ANALİZ VE BULGULAR

Çalışmanın istatistiksel analiz aşamasında frekans analizi, yapısal eşitlik modellemesi ile faktör analizi ve ortalama karşılaştırma testleri uygulanmıştır.

İlk aşamada katılımcıların demografik bulgularına göre frekans analizleri sunulmuştur. Frekans analizi bulgularından gruplara ait frekans (n) ve yüzde (%) değerleri birlikte gösterilmiştir.

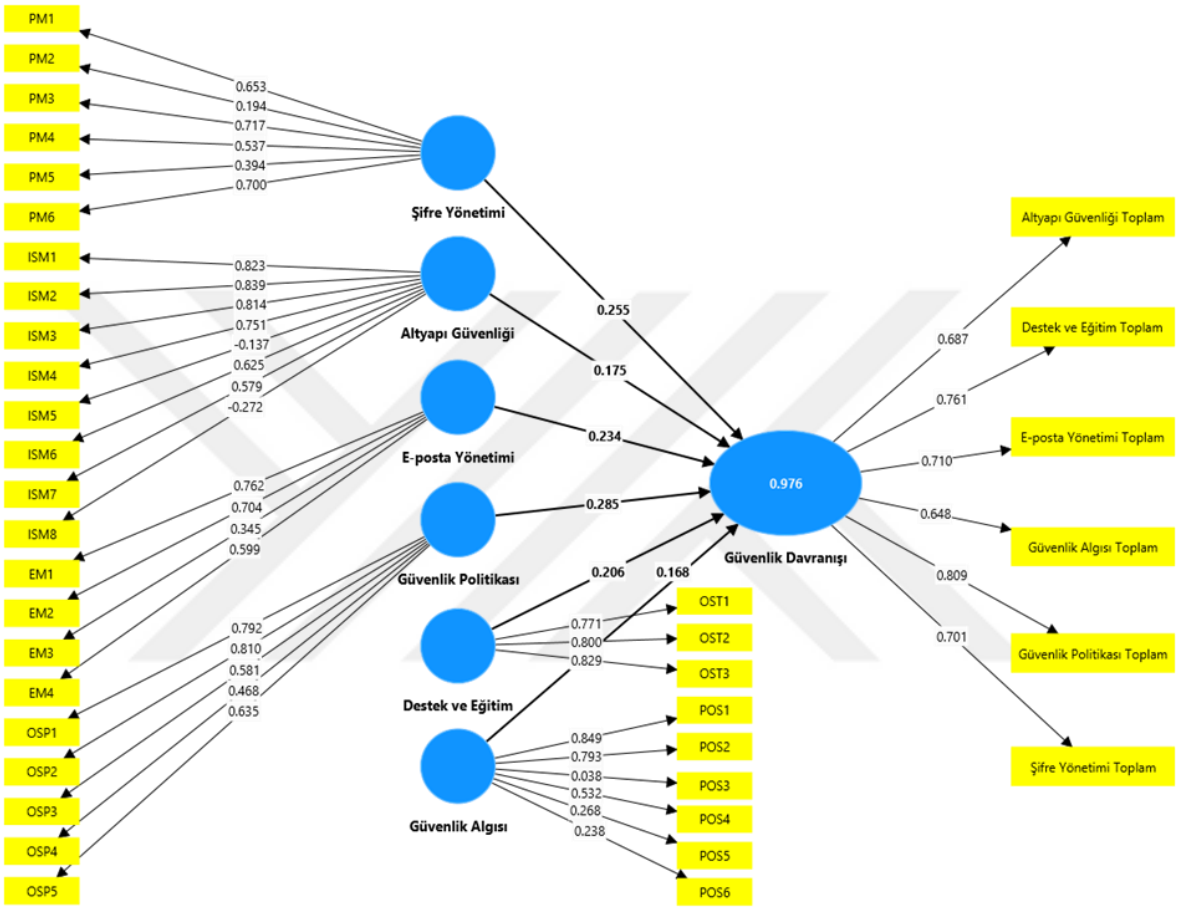
Tablo 3.1. Katılımcıların demografik özellikleri

Değişken	Grup	n	%
Çalışma şekliniz	Hibrit	214	68.9
	Uzaktan	106	31.1
Cinsiyet	Belirtmek istemiyorum	7	2.2
	Erkek	179	55.9
	Kadın	134	41.9
Yaş	24 yaş ve altı	30	9.4
	25-34	187	58.4
	35-44	57	17.8
	45-54	23	7.2
	54 yaş üzeri	23	7.2
Eğitim düzeyi	Lise ve altı	29	9.1
	Lisans derecesi	197	61.6
	Yüksek lisans derecesi	79	24.7
	Doktora derecesi	15	4.7

Tablo 3.1.'de katılımcıların demografik özelliklerine göre yapılan frekans analizi bulguları gösterilmektedir. Frekans analizi bulguları incelendiğinde, katılımcıların %68.9'unun hibrit, %31.1'inin ise uzaktan çalıştığı görülmektedir. Bu katılımcıların %2.2'si cinsiyetini belirtmezken, %55.9'u erkek, %41.9'u ise kadındır. Yaş düzeylerine göre katılımcıların %9.4'ü 24 yaş ve altı, %58.4'ü 25-34 yaş, %17.8'i 35-44 yaş, %7.2'si 45-54 yaş, %7.2'si ise 54 yaş üzerinde olduğu belirlenmiştir. Ayrıca katılımcıların %9.1'i lise ve altı, %61.6'sı lisans, %24.7'si yüksek lisans, %4.7'si ise doktora mezunudur.

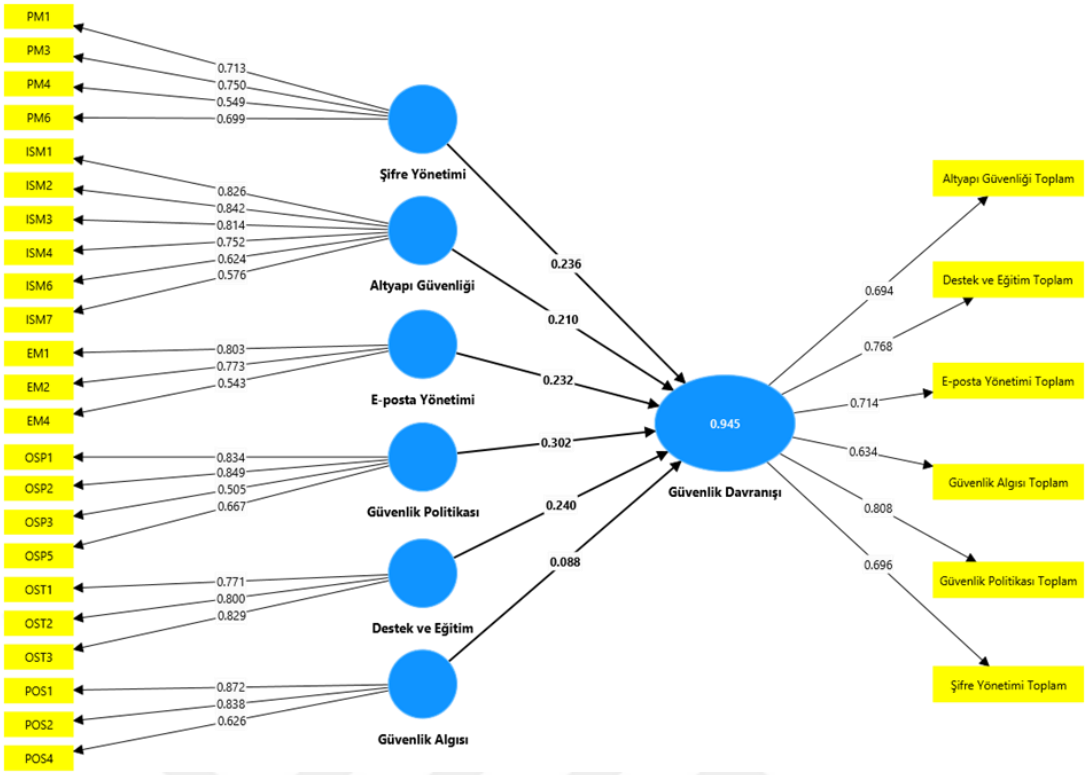
Ölçeğin alt boyutlarını belirlemek için yapısal eşitlik modellemesi ile faktör analizi uygulanmıştır (Şekil 3.1.). Faktör yükü 0.5'in altında olan maddeler (Pasaport

Management ‘Şifre Yönetimi’ PM2, PM5, Infrastructure Security Management ‘Altyapı Güvenliği Yönetim’ ISM5, ISM8, Email Management ‘Şifre Yönetimi’ EM3, Organizasyonel Security Policy ‘Kurumsal Güvenlik Politikası’ OSP4, Perception of Security ‘Güvenlik Algısı’ POS3, POS5, POS6) analiz dışında bırakılmış ve araştırma kapsamında sunulan değişkenler final model (Şekil 3.2.) üzerinden değerlendirilmiştir.



Şekil 3.1. Yapısal eşitlik modellemesi ile faktör analizi

Şekil 3.1.’de yapısal eşitlik modellemesi tekniği ile yapılan faktör analizi sonuçları gösterilmektedir. Her bir maddenin faktör yükünün anlamlı sayılması için ilgili faktör yükü değerlerinin 0.7 olması önerilmektedir. Ancak bu değer 0.2’ye kadar düşürülebilir (Saeed 2023). Çalışmamızda, faktör yükü 0.5’in altında olan maddeleri analiz dışında bırakılmıştır. Şekil 3.2.'de, faktör yükü 0.5'in altında olan maddeleri modelden çıkardıktan sonra yapılan yapısal eşitlik modellemesi ile faktör analizi sonuçları gösterilmektedir. Bulgular incelendiğinde, maddelerin faktör yükü değerlerinin 0.5’in üzerinde olduğu görülmektedir.



Şekil 3.2. Yapısal eşitlik modellemesi ile geliştirilmiş faktör analizi modeli

Model üzerinden yapılan güvenilirlik analizi sonuçlarına göre, Cronbach Alfa değerleri sırasıyla 0.620, 0.834, 0.611, 0.681, 0.719 ve 0.693 olarak bulunmuştur. Genel Cronbach Alfa değeri ise 0.814 olarak elde edilmiştir. Bu model üzerinden araştırmada belirlenen değşkenlerin değerlendirilmesi yapılmış ve sonuçlar Tablo 3.2.'de gösterilmiştir.

Tablo 3.2. Değişkenlerin sonuçları

Değişken	Örnek Ortalama	SS	T istatistiği	p değeri
Şifre Yönetimi	0.235	0.019	12.113	<0.001
Altyapı Güvenliği	0.209	0.020	10.676	<0.001
E-posta Yönetimi	0.231	0.022	10.774	<0.001
Güvenlik Politikası	0.302	0.020	14.981	<0.001
Destek ve Eğitim	0.238	0.023	10.274	<0.001
Güvenlik Algısı	0.089	0.019	4.756	<0.001

Tablo 3.2.'de Bulgular incelendiğinde, araştırma kapsamında oluşturulan faktörlerin onaylandığı görülmektedir ($p<0.05$). Bu durumda, etkili şifre yönetimi, altyapı güvenliği kaynaklarının etkili yönetimi, doğru e-posta yönetimi faaliyetleri, organizasyonel güvenli politikası, organizasyonel destek ve eğitim ile güvenlik algısının olumlu bilgi güvenliği davranışı üzerinde istatistiksel olarak anlamlı bir etkiye sahip olduğu gözlemlenmiştir.

Yapısal eşitlik modellemesi ile faktör analizi Smart PLS 4 paket programı kullanılarak gerçekleştirilmiştir. Diğer tüm analizler ise IBM SPSS 27 paket programı kullanılarak yapılmıştır.

Tablo 3.3. Katılımcıların demografik özelliklerine göre güvenlik davranışı düzeyleri

Değişken	Ort	SS	Medyan	IQR	Test ist	p
Çalışma şekli						
Hibrit	84.59	14.09	85.00	22.00	5.838	<0.001[T]
Uzaktan	74.06	14.21	74.00	19.00		
Cinsiyet						
Belirtmek istemiyorum[a]	96.14	15.83	97.00	23.00		
Erkek[a]	82.17	14.39	82.00	21.00	4.831	0.009[A]
Kadın[b]	79.46	15.39	78.50	21.00		
Yaş düzeyi						
24 yaş ve altı[ab]	82.90	14.24	84.50	26.00		
25-34[b]	79.73	15.49	80.00	22.00		
35-44[a]	86.68	14.59	89.00	25.00	10.499	0.033[K]
45-54[ab]	82.65	14.61	79.00	14.00		
54 yaş üzeri[b]	77.83	10.37	77.00	16.00		
Eğitim düzeyi						
Lise ve altı[a]	74.55	11.12	72.00	16.00		
Lisans derecesi[b]	81.60	14.62	82.00	21.00	9.891	0.020[K]
Yüksek lisans derecesi[b]	82.16	16.55	81.00	22.00		
Doktora derecesi[b]	86.67	15.69	85.00	27.00		

Ort: Ortalama, SS: Standarrt sapma, IQR: Çeyrekler arası açıklık,
T: Bağımsız örneklemler t testi, A: Anova testi, K: Kruskal Wallis testi,
a-b: Aynı harfler arasında farklılık yok

Tablo 3.3.'te araştırmaya katılan katılımcıların güvenlik davranışı düzeylerinin demografik özelliklere göre karşılaştırma testi sonuçları sunulmaktadır. Bulgular incelendiğinde, katılımcıların güvenlik davranışı düzeylerinin çalışma şekli, cinsiyet, yaş ve eğitim düzeylerine göre istatistiksel olarak anlamlı bir farklılık olduğu gözlemlenmiştir ($p<0.05$). Hibrit çalışan katılımcıların güvenlik davranışı düzeyleri, uzaktan çalışan katılımcılara göre daha yüksektir. Kadınların güvenlik davranışı düzeyleri, erkekler ve cinsiyetini belirtmek istemeyen katılımcılara göre daha düşüktür. Ayrıca 35-44 yaş aralığındaki katılımcıların güvenlik davranışı düzeyleri, 25-34 yaş ve 54 yaş üzerindeki katılımcılara göre daha yüksektir. Diğer taraftan, eğitim düzeyi lise ve altı olan katılımcıların güvenlik davranışı düzeylerinin lisans, yüksek lisans ve doktora mezunu olan katılımcılara göre daha düşüktür.

4. SONUÇ VE DEĞERLENDİRME

Araştırma, Türkiye'de uzaktan veya hibrit çalışma modelini benimseyen işletmelerde çalışan bireylerin bilgi güvenliği davranışlarını incelemektedir. Bu kapsamda, belirlenen alt boyut doğrultusunda katılımcılara anket uygulanmış ve elde edilen veriler istatistiksel yöntemlerle analiz edilmiştir.

Araştırmanın bulguları, etkili şifre yönetimi, altyapı güvenliği, uygun e-posta yönetimi, organizasyonel güvenlik politikaları, organizasyonel destek ve eğitim ile güvenlik algısının bilgi güvenliği davranışları üzerinde olumlu bir etkisi olduğunu ortaya koymaktadır. Ayrıca, demografik özelliklerin de bilgi güvenliği davranışları üzerinde anlamlı farklılıklar yarattığı belirlenmiştir. Çalışma sonucunda hibrit çalışanların bilgi güvenliği davranışları, uzaktan çalışanlara göre daha korumacı bulunmuştur. Bu, hibrit çalışmanın daha fazla yüz yüze etkileşim, ofis ortamında işletmenin bilgi güvenliği alt yapısının kullanılması ve organizasyonel kontrol ile ilişkilendirilebilir. Bunun yanı sıra katılımcıların demografik verilerine göre bilgi güvenliği davranışlarında da farklılıklar olduğu görülmüştür. Çalışmadan elde edilen bulgulara göre erkek katılımcıların güvenlik davranış düzeyleri, kadınlara göre daha yüksek olduğu görülmüştür. Bu sonuçlar bize cinsiyetin bilgi güvenliği farkındalığı ve davranışları üzerindeki etkisinin olduğunu göstermektedir. Katılımcıların yaş bilgilerine göre de bilgi güvenliği davranışlarında farklılaşma gözlemlenmiştir: 35-44 yaş aralığındaki katılımcıların güvenlik davranışlarının diğer yaş gruplarına göre daha yüksek olduğu sonucuna ulaşılmıştır. Orta yaş grubunun bilgi güvenliği konusunda daha deneyimli ve eğitimli olabileceği düşünülmektedir. Kemiksiz (2002) çalışmasında dijital yerlilerin kişisel veri güvenliği konusundaki tutumlarının göçmenlere göre daha dikkatsiz olduğunu belirtmiştir. Göçmenlerin ise daha tedbirli olduğu, ancak yerlilerin dijital yetkinliklerinin güvenlik risklerini anlamada yetersiz kaldığı vurgulanmıştır. Bu durum, çalışmanın yaş gruplarına yönelik bulguları ile örtüşmektedir. Ayrıca katılımcıların eğitim düzeyi arttıkça, bilgi güvenliği davranışlarının da olumlu yönde arttığı görülmüştür. Özellikle yüksek lisans ve doktora mezunları, daha yüksek güvenlik davranışına sahiptir. Daha önce yapılan çalışmalarda da bilgi güvenliği farkındalığının yaş ve eğitim düzeyi değiştikçe farklılaştığı tespit edilmiştir (Karapınar ve Daş, 2023).

Demografik verilerin güvenlik davranışları üzerine etkisinin yanı sıra çalışmada etkili şifre yönetimi, altyapı güvenliği, e-posta yönetimi, organizasyonel güvenlik politikaları, organizasyonel destek ve eğitim ve güvenlik algısının bilgi güvenliği davranışları üzerinde etkisi olup olmadığı belirlenen alt boyutlarla test edilmiştir.

Araştırmanın sonuçları, uzaktan ve hibrit çalışma ortamlarında bilgi güvenliğinin sağlanmasında kritik faktörleri belirlemiş ve bu faktörlerin çalışanların güvenlik davranışları üzerindeki etkilerini ortaya koymuştur. Bu bulgular, işletmelerin bilgi güvenliği politikalarını geliştirmelerine ve çalışanlarının güvenlik farkındalığını artırmalarına yönelik önemli ipuçları sunmaktadır. Ayrıca, demografik özelliklerin güvenlik davranışları üzerindeki etkisi, farklı çalışan gruplarına yönelik özel eğitim ve destek programlarının geliştirilmesi gerektiğini göstermektedir.

Bu araştırma, Türkiye'de uzaktan veya hibrit çalışanların bilgi güvenliği davranışlarını inceleyen ilk çalışma olmuştur, gelecekte yapılacak araştırmalar için de önemli bir temel oluşturmaktadır. İşletmeler, bu bulgular ışığında bilgi güvenliği stratejilerini gözden geçirerek, çalışanların güvenlik farkındalığını artırmak ve olası güvenlik risklerini minimize etmek için gerekli önlemleri almalıdır. Ayrıca, dijital dönüşüm süreçlerinde bilgi güvenliği kültürünün benimsenmesi ve çalışanların bu kültüre uyum sağlaması için sürekli eğitim ve farkındalık programlarının uygulanması önerilmektedir.

Ayrıca, Bilgi Güvenliği ve Çalışan Davranışı, organizasyonunuzu istenmeyen güvenlik ihlallerinin önlenmesine veya etkilerinin azaltılmasına olanak tanıyacak yetenek ve kültürü geliştirmenize yardımcı olacaktır.

Saeed 2023, yılında yayımlanan makalesinde ki alt başlıklarda Altyapı yönetimi, şifre yönetimi ve güvenlik algısı alt boyutlarında Suudi Arabistan'da yapılan ankette negatif sonuçlar çıkmıştır. Türkiye'de yaptığımız bu tez çalışmasında, aynı konuları ele alan alt boyutlar da davranışların olumlu olduğu sonucu çıkmıştır.

Araştırma, bilgi güvenliği davranışlarının geliştirilmesine yönelik somut öneriler sunarken, aynı zamanda uzaktan ve hibrit çalışma modellerinin yaygınlaştığı günümüzde, bilgi güvenliğinin korunmasının önemine dikkat çekmektedir. Değişen çalışma ortamında

etkili bilgi güvenliği uygulamalarının, kurumsal desteğin ve kapsamlı güvenlik politikalarına duyulan ihtiyacın önemini pekiştirir. Bu bulguların entegre edilmesi, uzaktan ve hibrit çalışma modellerindeki bilgi güvenliği davranışlarının anlaşılmasını geliştirebilir ve sonuçta daha güvenli ve üretken iş ortamlarına katkıda bulunabilir.

KAYNAKLAR

4cornerresources.2021. “How To Manage A Hybrid Workforce: Tips For Making Remote Teams Successful.” https://www.4cornerresources.com/blog/how-tomanage-a-hybrid-workforce-tips-for-makingremote-teams-successful/

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

Açıkgöz, B., ve Mutlu, M. D. (2022). Muhasebe Mesleğinde Dijital Dönüşüm: COVID-19 Pandemi Döneminde Uzaktan Çalışma Uygulamaları. İnsan ve Toplum Bilimleri Araştırmaları Dergisi, 11(2), 845-864.

Airtasker (2020, March 31). The Benefits of Working From Home

Akar, İ.Çalışma yaşamında yenilikler: Pandemi ile dijitalleşme deneyimi İlker Akar, Oytun Meçik Volume / Cilt: 8, Issue / Sayı: 4, 2021, pp. 403-411 E - ISSN: 2148-4139 URL: https://www.journals.gen.tr/jlecon DOI: https://doi.org/10.15637/jlecon.8.4.01

Akbaş Tuna, A., ve Türkmendağ, Z. (2020). Covid-19 Pandemi Döneminde Uzaktan Çalışma Uygulamaları ve Çalışma Motivasyonunu Etkileyen Faktörler. İşletme Araştırmaları Dergisi, 12(3), 3246-3260.

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

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

Al-Fedaghi, S., ve Alnasser, H. (2020). Modeling Network Security: Case Study of Email System. International Journal of Advanced Computer Science and Applications, 11(3), 99.

Alagöz A ve. Allahverdi M, (2011) Kurumsal Bilgi Güvenliği ve Muhasebe Bilgi Sistemi. (Muhasebe ve Vergi Uygulamaları Dergisi Cilt: 4 Sayı: 3, 47- 64).

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Understanding Information Security Management in the Context of Organizational Culture: A Conceptual Framework. In

Proceedings of the 8th Australasian Information Security Conference (AISC 2010) (pp. 47-55). Brisbane, Australia. https://doi.org/10.5555/1862266.1862275

Allen, N. J., ve Meyer, J. P. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. Journal of Occupational Psychology, 63, 1–18.

Alqahtani, M. A. (2022). Cybersecurity Awareness Based on Software and E-mail Security with Statistical Analysis. Computational Intelligence and Neuroscience, Volume 2022, Article ID 6775980, 12 pages. https://doi.org/10.1155/2022/6775980

Alshaikh, M., Maynard, S. B., Ahmad, A., ve Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations.

Altıntaş, S., ve Barkuş, F. (2023). Dijital Ortamlarda Kişisel Veri Güvenliği Kavramı Üzerine Bir Derleme Çalışması. Electronic Journal of Vocational Colleges, 13, 46-69.

Anderson, R. M., Fraser, C., Ghani, A. C., Donnelly, C. A., Riley, S., Ferguson, N. M., ... ve Hedley, A. J. (2004). Epidemiology, transmission dynamics and control of SARS: the 2002–2003 epidemic. Philosophical Transactions of the Royal Society of London. Series B: Biological Sciences, 359(1447), 1091-1105

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

Arregi, A., Gago, M., ve Legarra, M. (2022). Employee Perceptions About Participation in Decision-Making in the COVID Era and Its Impact on Psychological Outcomes: A Case Study of a Cooperative in MONDRAGON (Basque Country, Spain). Sustainability, 13.

Assunção, P. (2019, January, 16-16). A zero trust approach to network security, Proceedings of the Digital Privacy and Security Conference. Portugal, 65-72. https://doi.org/10.11228/dpsc.01.01.007

B. Alkhazi, M. Alshaikh, S. Alkhezi and H. Labbaci, "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and

Behavior," in IEEE Access, vol. 10, pp. 132132-132143, 2022, doi: 10.1109/ACCESS.2022.3230286.

Bahadır, Z. (2017). Beyaz Yakalılar: Kol Gücüne Dayanmayan Kafa Gücüne Dayanan Büro İşçileri. Ahi Evran Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 1(1), 129-134.

Banita, L., ve Dwivedi, Y. K. (2009). Homeworkers' usage of mobile phones; social isolation in the home- workplace. Journal of Enterprise Information Management, 22(3), 257-274.

Banjo, S., Yap, L., Murphy, C., Chan, V., 2020, The Coronavirus Outbreak Has Become the World's Largest Work-From-Home Experiment.

Barsness, Z. I., Diekmann, K. A., ve Seidel, M.-D. L. (2005). Motivation and Opportunity: The Role of Remote Work, Demographic Dissimilarity, and Social Network Centrality in Impression Management. Academy of Management Journal, 48(3), 401–419.doi:10.5465/amj.2005.17407906

Bartik, A. W., Bertrand, M., Cullen, Z., Glaeser, E., Luca, M., ve Stanton, C. (2020). How are small businesses adjusting to Covid-19? Early evidence from a survey. Cambridge, UK: National Bureau of Economic Research.

Başol, G., ve Çömlekçi, C. (2021). Sosyal ve demografik değişkenler ile uzaktan çalışma arasındaki ilişki: Türkiye beyaz yakalı çalışanları üzerine bir araştırma. İşletme Araştırmaları Dergisi, 13(2), 506-531.

Baykara, M., Daş, R., Karadoğan, İ. (2013). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, *1. st International Symposium on Digital Forensics and Security* (ISDFS'13), 20-21 May 2013, Elazığ, Turkey 231.

Bellinger, G., Castro, D., ve Mills, A. (2004). Data, information, knowledge, and wisdom.

Beňo, M. (2021). The advantages and disadvantages of E-working: An examination using an ALDINE analysis. Emerging Science Journal, 5(1), 11-20.

Bhat, S. K., Pande, N., ve Ahuja, V. (2016). Virtual Team Effectiveness: An Empirical Study using SEM. International Journal of Virtual and Personal Learning Environments (IJVPLE), 6(1), 1-17.

Bilginoğlu, E. (2021). COVID-19 pandemisi sırasında uzaktan çalışmanın artan önemi: Bilinen yanlışlar ve doğruları. Çalışma ve Toplum, 2(69), 1099-1146. Bilimler Kongresi ile Sağlık, Mühendislik ve Uygulamalı Bilimler Kongresi 28-30 Eylül 2023).

Bodepudi, A. And Reddy, M. (2021) The Rise of Virtual Employee Monitoring in Cloud andIts Impact on Hybrid Work Choice (SageScience publishingJournal of Artificial Intelligenceand Machine Learning in Management).

Borg, Cornelia ve O'Sullivan, Caoimhe, "The Corporate Brand Identity in a Hybrid Workplace Model", Yüksek Lisans Tezi. Lund Üniversitesi, 2021.

Brynjolfsson, E., Horton, J., Ozimek, A., Rock, D., Sharma, G., ve TuYe, H.-Y. (2020). COVID-19 and Remote Work: An Early Look at US Data. National Bureau of Economic Research, doi:10.3386/w27344

Cai, H., Gan, C., Wang, T., Zhang, Z., ve Han, S. (2019). Once-for-all: Train one network and specialize it for efficient deployment. arXiv preprint arXiv:1908.09791.

Cavusoglu, H., Cavusoglu, H., ve 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.

Chan, M., Woon, I., ve 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.

Cheng, M. Y., Ho, J. S. Y., ve 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., ve Bloodgood, J. M. (2008). The dimensions of tacit ve 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., ve 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.

Civan Kemiksiz, R. (2022). Büyük Veri Çağında Kişisel Veri Güvenliği Üzerine Bir Alan Araştırması: Dijital Yerliler ve Dijital Göçmenlerin Güvenlik Algıları. Maltepe Üniversitesi İletişim Fakültesi Dergisi, 9(1), 64-91.

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

Cooper, C. D., ve Kurland, N. B. (2002). Telecommuting, professional isolation, and employee development in public and private organizations. Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior, 23(4), 511-532.

Çakmak Karapınar, D., ve Daş, A. (2023). Açık ve uzaktan eğitim öğrencilerinin bilgi güvenliği farkındalığı: Atatürk Üniversitesi örneği. Yıl 2023, Sayı: 93, ss. 103-118, 16.03.2023. DOI: https://doi.org/10.17753/sosekev.1148987

Çalışanların Bilgi Güvenliği Önlemlerine Dair Tutumları: Ampirik Bir Değerlendirme* http://www.ijaefs.com/wp-content/uploads/2022/12/02_ECE-CAKMAK.pdf

Çek, E. (2020). "Kurumsal Bilgi Güvenliği Yönetişimi ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi." İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı Tezi.

Daston L, (2017) KNOW: A Journal on the Formation of Knowledge (Volume 1, Number 1Spring 2017 Reflections on Disciplinary Knowledge).

Deloitte. (2020). İşin Geleceği: Uzaktan çalışma sisteminde organizasyonel dayanıklılığı korumak, Deloitte Raporu.

Demir, N. (2008). Örgütlerin Etik Kültürü ve Beyaz Yakalı Çalışanların Pazarlama Etik Anlayışını İrdeleyen Bir Saha Çalışması. Öneri Dergisi, 8(29), 139-145.

Demirel Değirmenci, S. (2022). Covid 19 Pandemisiyle Zorunlu Esnek Çalışma ve Teknoloji Eliyle Denetim. Turkish Online Journal of Design Art and Communication, 12(4), 1140-1151.

Develioğlu, H. M. (2018). Avrupa Birliği Genel Veri Koruma Tüzüğü. İstanbul: On İki Levha Yay. Erişim adresi: onikilevha.com.tr

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

Doğan, O., ve Aşan, H. (2016). Bireylerin Şifre Yapılarına Yönelik Bir Araştırma ve Şifre Öneri Sistemi. Adıge Bilim Dergisi, 1(3), 192-201 https://doi.org/10.12345/abcd.12345

Donna Zeller. (2018). Organizational Design: The Hybrid (Virtual Offsite / Traditional 'Brick andMortar')Organization(Summer2018).Zenodo. https://doi.org/10.5281/zenodo.1306781

Ecek, N., & Çakmak, A. F. (2022). Çalışanların Bilgi Güvenliği Önlemlerine Dair Tutumları: Ampirik Bir Değerlendirme. International Journal of Applied Economic and Finance Studies, 7(2), 26-44.

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

Erdayı, A. U. (2012). Beyaz yakalıların tanımlanması üzerine. "İş, Güç" Endüstri İlişkileri ve İnsan Kaynakları Dergisi, 14 (3), 65–80.

Esteve-Gonzalez, P., Dutton, W. H., Creese, S., ve Agrafiotis, I. (2023). Cybersecurity implications of changing patterns of office, home, and hybrid work: An exploratory global survey. Home, and Hybrid Work: An Exploratory Global Survey (January 11, 2023).

Eurostat. "Key Figures on the Impact of the COVID-19 Crisis on the Labour Market", 2021.

Fayard, A. L., Weeks, J., ve Khan, M. (2021). Designing the Hybrid Office. Harvard Business Review, 1-11.

Figueroa III, J. D. (2022). Information Security Compliance Intention Within Remote and Hybrid Work Environments (Doctoral dissertation, Universidad Ana G Méndez-Gurabo).

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

Galanti, T., Guidetti, G., Mazzei, E., Zappalà, S., ve Toscano, F. (2021). Work from home during the COVID-19 outbreak: the impact on employees' remote work productivity, engagement, and stress. Journal of occupational and environmental medicine, 63(7), 426-432.

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

Ganal, S., Yalçınkaya, M. A., ve Küçüksille, E. U. (2017). "Kurumsal Bilgi Güvenliği Üzerinde Yeni Kayıtlı İnternet Sitelerinin Etkisinin Analiz Edilmesi." Süleyman Demirel Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü.

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

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

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

Gurung, A.; Luo, X.; Liao, Q. Consumer motivations in taking action against spyware: An empirical investigation. Inf. Manag. Comput. Secur. 2009, 17, 276–289.

Gülmüş, M. (2010) Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği Yıldız Teknik üniversitesi Fen Bilimleri enstitüsü, Yüksek Lisans Tezi.

Günay, E. K., ve Torgalöz, A. Ö. (2020). Covid-19 Sürecinde Türkiye'de Uzaktan Çalışma ve İstihdamdaki Dönüşüm. Uluslararası Akademik Araştırmalar Kongresi, 404-412.

Gürbüzoğlu, E. Ö., ve Ekici Gürbüzoğlu, Y. (2019). Beyaz Yakalı Çalışanlarda Aranan Becerilerin Belirlenmesine Yönelik Bir Araştırma. International Journal of Management and Administration, 3(5), 149-160.

Han, D., Dai, Y., Han, T., ve 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.

Harpaz, I. (2002). Advantages and disadvantages of telecommuting for the individual, organization and society. Work study, 51(2), 74-80.

Hart, S., Margheri, A., Paci, F., ve Sassone, V. (2021). Riskio: A Serious Game for Cyber Security Awareness and Education. Computers ve Security, 104, 102178.

Hekimler, A. (2022). Pandemi Sürecinde Home Office–Uzaktan Çalışma-ve Çalışma Yaşamının Geleceği. Balkan ve Near Eastern Journal of Social Sciences (BNEJSS), 8(2).

Hertel, G., Geister, S., ve Konradt, U. (2005). Managing virtual teams: A review of current empirical research. Human resource management review, 15(1), 69-95.

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

IWG Workplace Survey (2019). "The IWG Workplace Survey 2019 provides valuable insights into the growing trend of flexible working and its impact on productivity and employee satisfaction (IWG, 2019)."

IWG Workplace Survey 2019: "The IWG Workplace Survey 2019 provides valuable insights into the growing trend of flexible working and its impact on productivity and employee satisfaction (IWG, 2019)."

İnce, D., ve Akbalık, S. (2022). Kamu Hastanelerinde Temizlik İşçilerinin Çalışma Koşulları ve Covid-19 Pandemi Sürecindeki Deneyimleri: İstanbul Örneği. Çalışma ve Toplum, 5(75), 2839-2873.

İşman, A. (2001). Teknolojinin felsefi temelleri. Sakarya Üniversitesi Eğitim Fakültesi Dergisi, (1).

Jalali, M. S., Landman, A., ve Gordon, W. J. (2021). Telemedicine, privacy, and information security in the age of COVID-19. Journal of the American Medical Informatics Association, 28(3), 671–672. https://doi.org/10.1093/jamia/ocaa310

Jouini, M., Rabai, L. B. A., ve 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.

Karabacak, B., ve Özkan, S. (2010). Bilgi Güvenliği Yönetim Sistemi için Süreç Tabanlı Risk Analizi. Ağ ve Bilgi Güvenliği Sempozyumu, Ankara, 5-6 Şubat 2010. Enformatik Enstitüsü, Orta Doğu Teknik Üniversitesi, Ankara.

Kayra, F. (2022). Sanal Liderlik ve Sanal Takımlar: Bir Derleme ve Değerlendirme. Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi, 23(2), 288-319.

Keser, A., ve Bilir, K. B. Ö. (2019). İş Tatmini Ölçeğinin Türkçe Güvenilirlik Ve Geçerlilik Çalişmasi. Kırklareli Üniversitesi Sosyal Bilimler Dergisi, 3(3), 229-239.

Keser, H. Ve Can, G. (2015). Development Of Information Security Awareness Scale. Ankara Üniversitesi, Eğitim Bilimleri Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Cebeci, Ankara (K. Ü. Kastamonu Eğitim Dergisi, 23 (3), 1167-1184).

Khudaykulov, A., Zheng, C. J., ..., ve Jakhongirov, I. (2022). The Fear of COVID-19 and Job Insecurity Impact on Depression and Anxiety: An Empirical Study in China in the COVID-19 Pandemic Aftermath. Frontiers in Psychology, 13

Kıcır, B. (2019). Evden Çalışma: Özgürlük Mü Esaret Mi?. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 21(1), 173-196.

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

King's College London. 2021. "New Ways of Working: The Lasting Impact and Influence of the Pandemic." https://www.kcl.ac.uk/giwl/assets/New-ways-ofworking.pdf

Knapp, K.J.; Morris Jr, R.F.; Marshall, T.E.; Byrd, T.A. Information security policy: An organizational-level process model. Comput. Secur. 2009, 28, 493–508

Kniffin, K. M. ve diğer., (2021). Covid-19 and the workplace: Implications, issues, and insights for future research and action. The American Psychologist. Advance online publication. 76 (1), 63-77. doi: 10.1037/amp0000716

Koçyiğit, N., ve Şendoğdu, A. A. (2022). İnsan Kaynakları Yönetimlerinin İşe Alım Kararlarında Vasıfsal İkilem. MANAS Sosyal Araştırmalar Dergisi, 11(3), 1137-1151.

Koushik, P.; Chandrashekhar, A.M.; Takkalakaki, J. Information security threats, awareness and cognizance. Int. J. Tech. Res. Eng. 2015, 2, 19–28.

Koyuncu, O. (2021). Yeni Normal Dünya Düzeninin Siber Güvenlik Ve Bilgi Güvenliğine Etkileri. (Yönetim Bilişim Sistemleri Dergisi Cilt:7 Sayı:1).

KSÜ Fen ve Mühendislik Dergisi, 11(1), 2008 KSU Journal 132 of Science and Engineering, 11(1), 2008 Bilgi Güvenliği Yönetimi Mehmet TEKEREK KSÜ, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Kahramanmaraş Geliş Tarihi: 12.12.2006 Kabul Tarihi: 22.05.2007

Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği Gülmüş, MustafaURI: http://localhost:6060/xmlui/handle/1/7782 Yıldız Teknik Üniversitesi Fen Bilimleri YL Tezi

Lee, S., Park, N. E., ve Suk, J. (2019). The Effects of Consumers' Information Security Behavior and Information Privacy Concerns on Usage of IoT Technology. Interacción '19: Proceedings of the XX International Conference on Human Computer Interaction, 54, 1–2. https://doi.org/10.1145/3335595.3335600

Liebowitz, J., ve 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.

Liebowitz, J., ve 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.

Lipnack, J., ve Stamps, J. (2010). Leading Virtual Teams: Expert Solutions to Everyday Challenges;[empower Members, Understand the Technology, Build Team Identity].

M. Jain, A. Sinha, A. Agrawal and N. Yadav, "Cyber security: Current threats, challenges, and prevention methods," 2022 International Conference on Advances in Computing, Communication and Materials (ICACCM), Dehradun, India, 2022, pp. 1-9, doi: 10.1109/ICACCM56405.2022.10009154.

Malecki, F. (2020). Overcoming the security risks of remote working. Computer fraud ve security, 2020(7), 10-12.

Mayer, P., Kunz, A., ve Volkamer, M. (2017). Reliable Behavioural Factors in the Information Security Context. ARES '17: Proceedings of the 12th International

Conference on Availability, Reliability and Security, August 2017, Article No.: 9, pp. 1–10. DOI: https://doi.org/10.1145/3098954.3098986

Mayrhofer, C., The Office Workplace of the Future: Virtual, Physical or Both?, Yayımlanmış Yüksek Lisans Tezi, Leopold-Franzens-Universität Innsbruck, 2021.

McIlwraith, A. (2021). Information security and employee behaviour: how to reduce risk through employee education, training and awareness. Routledge.

Mercan, N. (2015). Ajzen'in Planlanmış Davranış Teorisi Bağlamında Whıstleblowıng (Bilgi İfşası). Sosyal ve Beşeri Bilimleri Dergisi, 7(2).

Mortenson, M. ve Haas, M. (2021). Making the Hybrid Workplace Fair. Harvard Business Review, https://hbr.org/2021/02/making-the-hybridworkplace-fair

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

Naser Alraja, M. Javed Butt, U. Abbod M. (2023) Information Security Policies Compliance İn A Global Setting: An Employeeve#39;s Perspective. https://doi.org/10.1016/j.cose.2023.103208

Nguyen, Q. C., Yardi, I., ..., ve Yue, X. H. (2022). Leveraging 13 Million Responses to the US COVID-19 Trends and Impact Survey to Examine Vaccine Hesitancy, Vaccination, and Mask Wearing, January 2021-February 2022. Journal of Medical Internet Research, 22(1).

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

Nowacki, K., Grabowska, S., ve Lis, T. (2021). The Impact of Remote Working During the COVID-19 Epidemic on Employee Well-being. Multidisciplinary Aspects of Production Engineering, 4(1), 245-254.

Nwankpa, K. J. ve Datta, P. M., (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. https://doi.org/10.1016/j.cose.2023.103266

O'Reilly, C. A., ve Chatman, J. (1986). Organizational commitment and psychological attachment: The effects of compliance, identification, and internalization on prosocial behavior. Journal of applied psychology, 71(3), 492.

Ogbanuge, O. E. Crossler, R. Biros, D. (2023). The valued coexistence of protection motivation and stewardship in information security behaviors. (Computers veamp; Security 124 (2023) 102960).

Olson, M. H. (1983). Remote office work: changing work patterns in space and time. Communications of the ACM, 26(3), 182–187.

Orhan, G., ve Karlıdağ, S. (2022). COVID-19 Günlerinde İstanbul'da Yürümek: Üniversite Eğitimli Çalışanlar Örneği. İDEALKENT, 14(Özel Sayı), 404-432. doi: 10.31198/idealkent.1066289

Orhan, M. A., Rijsman, J. B., van Dijk, G. M. (2016), Invisible, Therefore Isolated: Comparative Effects of Team Virtuality with Task Virtuality on Workplace Isolation and Work Outcomes", Journal of Work and Organizational Psychology, Vol 32, s. 109-122.

Ortiz-Prado, E., Simbaña-Rivera, K., Barreno, L. G., Diaz, A. M., Barreto, A., Moyano, C., ... ve Lowe, R. (2021). Epidemiological, socio-demographic and clinical features of the early phase of the COVID-19 epidemic in Ecuador. PLoS neglected tropical diseases, 15(1), e0008958.

Özalp, Z. (2020). Covid-19 Bağlamında Devletlerin Hak ve Sorumlulukları. Sosyal Bilimler Araştırma Dergisi, 9(2), 127-132.

Özay,B. (2022). Covid-19 Küresel Salgını Etkisiyle Türkiye ve Dünyada Uzaktan Çalışma ve İstihdam Yöntemlerindeki Değişimler. VI. Anadolu International Conference on Economics May 13-15, 2022, Eskişehir, Turkey.

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

Özdemir, H. Ö., ve Erkutlu, H. V. (2017). Yöneticilerin otantik liderlik tarzlarının çalışanların sanal kaytarma ve sinizm davranışları üzerine etkileri.

Özerdem, A. (2021) SİHA'ların Kullanımında Etik Boyut ORCID: 0000-0001-7447-096X DOI: 10.36484/liberal.1018568 Liberal Düşünce Dergisi, Yıl: 26, Sayı:104, Güz 2021, ss.145-162. Gönderim Tarihi: 3 Kasım 2021 | Kabul Tarihi: 25 Kasım 2021

Öztürkoğlu, Y. (2013). Tüm Yönleriyle Esnek Çalışma Modelleri, Beykoz Akademi Dergisi, 1(1), 109-129.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., ve 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.

Pathak, E. B., Menard, J. M., ..., ve Salemi, J. L. (2022). Joint Effects of Socioeconomic Position, Race/Ethnicity, and Gender on COVID-19 Mortality Among Working-Age Adults in the United States. Ethnicity ve Disease, 19(9).

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

Radonić, M., Vukmirović, V., ve Milosavljević, M. (2021). The impact of hybrid workplace models on intangible assets: The case of an emerging country. Amfiteatru economic, 23(58), 770-786.

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

Saeed, S. (2023). DigitalWorkplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. (Sustainability 2023, 15, 6019. https://doi.org/10.3390/su15076019)

Safa, N. S., Von Solms, R., ve Furnell, S. (2016). Information security policy compliance model in organizations. computers ve security, 56, 70-82.

Savić, D. (2020). COVID-19 Work from Digital Transformation of the Workforce. The Grey Journal, 16(2), 101-104.

Scardamalia, M., ve Bereiter, C. (2010). A Brief History of Knowledge Building. Canadian Journal of Learning and Technology, 36(1). https://www.cjlt.ca/index.php/cjlt/article/view/548

Senapati, S., ve Bharathi, S. V. (2024). An Empirical Study on the Information Security Threats Due to Remote Working Environments. Conference paper, First Online: 03 January 2024.Senapati, S. ve Bharathi, S.V.

Seyfikli, C. (2007). Hastane yöneticilerinin liderlik davranışlarının personel iş doyumuna etkisi (Master's thesis, Sosyal Bilimler Enstitüsü).

Shimura, A., Yokoi, K., Ishibashi, Y., Akatsuka, Y., ve Inoue, T. (2021). Remote work decreases psychological and physical stress responses, but full-remote work increases presenteeism. Frontiers in Psychology, 4190.

Siber Güvenlik Politikalarının Karşılaştırılmalı Bir Analizi İngiltere ve Türkiye Örneği ISBN:9782382365625, 2382365625 Sayfa sayısı:241 Yayınlanma Tarihi:20 Haziran 2023 Biçim:E-kitap Yayıncı:Livre de Lyon Dil:Türkçe Yazar:Gül Nazik ÜNVER syf118.

Siponen, M., Pahnila, S., ve 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.

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.

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.

Sokale, I., Alvarez, J., ve Oluyomi, A. O. (2022). COVID-19 Vaccine Uptake Among US Adults According to Standard Occupational Groups. Journal of Community Health, 10(7).

Soysal, T. (2006). Tele Çalışma, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, 9, 2006/1, 133–165.

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

Şahin, M. D., Söylemez, E. Y., ve Koç, Y. D. (2016). Planlanmış Davranış Teorisi Çerçevesinde Aile İşletmelerinde Kurumsallaşma Sürecinin İrdelenmesi. Dumlupınar Üniversitesi Sosyal Bilimler Dergisi / Dumlupınar University Journal of Social Sciences Afro-Avrasya Özel Sayısı-Aralık 2016 / Special number of Afro-Eurasia-December 2016.Şahin,

Şakar, M., ve Şahin, D. E. (2021). Esnek Çalışma Modellerinden Uzaktan Çalışma ve Uzaktan Çalışanların Sigortalılığı. SGD-Sosyal Güvenlik Dergisi, 11(2), 249-267. DOI: 10.32331/sgd.1048957

Şakar, M., ve Şahin, D. E. (2021). Esnek çalışma modellerinden uzaktan çalışma ve uzaktan çalışanların sigortalılığı. SGD-Sosyal Güvenlik Dergisi, 11(2), 249-267.

Şanlısoy, S. (2016). Bilgi Toplumunda Ortaya Çıkabilecek Sorunlar. Dokuz Eylül Üniversitesi İktisadi İdari Bilimler Fakültesi Dergisi, 14(2).

Taboroši, S., Strukan, E., Poštin, J., Konjikušić, M., ve Nikolić, M. (2020). Organizaciona posvećenost i poverenje zaposlenih na daljinu. Journal of Engineering Management and Competitiveness (JEMC), 10(1), 48-60. https://doi.org/10.5937/jemc2001048T

Tağraf, H., ve Çalman, İ. (2009). OHİO üniversitesi liderlik modeline göre oluşan liderlik biçimlerinin işletmelerin ihracat performansı üzerine etkisi ve gaziantep ilinde bir araştırma. Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi, 23(2), 135-154.

Taras Shevchenko 6th Internatıonal Congress On Socıal Scıences.

Taş, A., Özkara, Z. U., ve Aydıntan, B. (2020). Elektronik Liderliğin Temel Boyutu: Sanal Teknoloji Yeterliğinin Yöneticiye Duyulan Güvene Etkileri. İşletme Araştırmaları Dergisi, 12(3), 2879-2894.

Taştan, N. S., ve Taştan, K. (2022). Uzaktan Çalışmada Yönetsel Konular Kitap İncelemesi. Turkish Management Review, 1(1), 63-65.

Tavares, A. I. (2017). Telework and health effects review. International Journal of Healthcare, 3(2), 30. https://doi.org/10.5430/ijh.v3n2p30

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

Thoughtexchange. 2021. "3 Steps for a Hybrid Workplace Your People (and Profits) Will Love." https://www.thoughtexchange.com/blog/what-isa-hybrid-workplace/

Toduk, Y. (2023). Lideri dijital çağın liderlik sırları. İstanbul: Doğan Egmont Yayınları.

Toffler, A. (1983). Previews and Premises. New York: William Morrow and Company.

Tozlu, E. (2011). Genel Olarak Esnek Çalışma Sistemleri ve Tele Çalışma ve Sıkıştırılmış İş Haftasının Karşılaştırılması, Süleyman Demirel Üniversitesi Vizyoner Dergisi, Y.2011, C.3, S.4. s.99-116

Triyason, T., Tassanaviboon, A., ve Kanthamanon, P. (2020). Hybrid Classroom: Designing for the New Normal after COVID-19 Pandemic, Proceedings of the 11th International Conference on Advances in Information Technology, https://doi.org/10.1145/3406601.3406635

Tuna, A. A., ve Türkmendağ, Z. (2020). Covid-19 pandemi döneminde uzaktan çalışma uygulamaları ve çalışma motivasyonunu etkileyen faktörler. İşletme Araştırmaları Dergisi, 12(3), 3246-3260.

Uçar, Z. ve Tutgaç, C. (2022). İşgörenlerin Dijital Okuryazarlık Algısı ve Dijital TeknolojilereErişim Motivasyonu İlişkisi Üzerinde Dijital Liderliğin Düzenleyicilik Rolü. İzmir Yönetim Dergisi, 3(1), 8-22.

Uluslararası Çalışma Örgütü (ILO). 2020. "COVID-19 Ortamında ve Sonrasında Uzaktan Çalışma." https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---iloankara/documents/publication/wcms_759299.pdf

Uysal, N., ve Yılmaz, M. Ç. (2020). Akademisyenlerde İş Yaşam Dengesi ve Uzaktan Çalışmaya İlişkin Görüşlerin Belirlenmesi. Uluslararası Sosyal Bilimler Akademik Araştırmalar Dergisi, 4(2), 26-37.

Vaughn, R. B., Dampier, D. A., ve Warkentin, M. B. (2004). Building an information security education program. InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development, October 2004, pp. 41–45. DOI: https://doi.org/10.1145/1059524.1059533

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

Vural, Y., ve Sağıroğlu, Ş. (2011). "Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler." Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, Cilt 26, No 1, 89-103.

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

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

Workinsync. 2020. "Hybrid Workplace Model: A Transition to New Normal of Work." https://www.workinsync.io/hybrid-workplacemodel-a-transition-to-the-new-normal-of-work/

Xie, J. L., Elangovan, A. R., Hu, J., ve Hrabluik, C. (2018). Charting new terrain in work design: a study of hybrid work characteristics. Applied Psychology. https://doi.org/10.1111/apps.12169

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

Yalçın, M. Ve Z. Beril, A.V (2021). Covid-19 Pandemisinde Uzaktan Çalışma ve Kurumsal Aidiyet: Akademisyenler Üzerine Bir Araştırma (Ata İlet Derg, 2021; Özel Sayı: 129-139).

Yel T, Atasoy A. (2021). Dijitalleşmenin Bağımsız Denetime Yansımalarının Siber Güvenlik Yönünden Değerlendirilmesi. Muhasebe ve Finansman Dergisi – Ağustos 2021 Özel Sayı.

Yerby, J., ve 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.

Yılmaz, M. (2009). Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi. Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi, 49(1), 95-118.

Zagzebski, L. (2017). What is Knowledge? In J. Greco ve E. Sosa (Eds.), The Blackwell Guide to Epistemology (s. Chapter 3). https://doi.org/10.1002/9781405164863.ch3

Zeller, D. (2018). Organizational Management in the Hybrid (combined virtual offsite/traditional 'brick and mortar') Transnational Organizations, The Pennsylvania State University.

Zengin,N. (2023) Dijital Dönüşümün İşletmeler Üzerindeki Etkileri: Dijital İş Modelleri Üzerinde Bir Araştırma. (8.Socrates Uluslararası Eğitim, İşletme, Ekonomi ve Sosyal

Zeybekoğlu, Ö. A., ve Dursun, C. (2020). Koronavirüs (covid-19) pandemisi sürecinde özel alanina kamusal alani siğdiran çalişan anneler. Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi, 7(5), 78-94.

Zhen, J. Dong,K. Xie, Z. Chen, L. (2022) Factors Influencing Employees' Information Security Awareness in the Telework Environment. (Electronics 2022, 11, 3458).

EKLER

EK-1: Anket Soruları

1)Çalışma şekliniz nedir?

Uzaktan
Hibrit

2)Cinsiyetiniz?

Erkek
Kadın
Belirtmek istemiyorum

3)Yaşınız?

18 yaş altı
18-24
25-34
35-44
45-54
54'ün üzerinde

4)Eğitim seviyeniz?

Lise diplomasından daha az
Lise diploması veya eşdeğer derece
Lisans derecesi
Yüksek lisans derecesi
Doktora derecesi

5)Şirketinizin çalışma alanı?

Bilişim Teknoloji
Danışmanlık
Eğitim
Savunma Havacılık
Enerji Doğal Kaynak
Finans
Gıda Tarım Hayvancılık
İnşaat Yapı Mimarlık Gayrimenkul
Kar Amacı Gütmeyen Kuruluş
Kimya Boya
Makine
Medya İletişim
Metal Çelik
Otomotiv

Perakendecilik
Sağlık İlaç Medikal
Spor
Lojistik Taşımacılık
Tekstil
Telekomünikasyon
Turizm Seyahat
Diğer:

6)Birden fazla sisteme erişmek için aynı şifreyi kullanıyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

7)Şirket politikası sebebi ile sık sık şifremi değiştiriyorum

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

8)Şifremi değiştirdiğimde eski şifremi temel alıyorum.

Kesinlikle Katılıyorum
Katılıyorum
Kararsızım
Katılmıyorum
Kesinlikle Katılmıyorum

9)Kullanıcı adımı/şifrelerimi bilgisayarımda saklıyorum veya bir yere not alıyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

10)Şifrelerimi takip etmek için bir yazılım kullanıyorum

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

11)Şifremi iş arkadaşlarımla paylaşıyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

12)Kişisel bilgisayarımda antivirüs programı yüklüdür.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

13)Antivirüs programı düzenli olarak güncellenmektedir.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

14)Bilgisayarımda kurulu bir güvenlik duvarı vardır.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

15)Bilgisayarımda casus yazılım önleme aracı kullanıyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

16)Bilgisayarımda " kod yazmaya" izin veriyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

17)Bilgisayardan uzaklaştığım zaman her zaman oturumu kapatıyorum veya bilgisayarı kilitliyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

18)Bilgisayarımda şifre korumalı bir ekran koruyucu kullanıyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

19)İş bilgisayarımda sosyal/profesyonel ağ sitelerini kullanıyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

20)Gönderenin kim olduğunu bilmesem bile e-postaları açıyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

21)Göndereni bilmediğim e-postaların eklerini de açıyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

22)E-posta gönderirken şifreleme kullanıyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

23)Web tabanlı e-posta veya takvim yazılımlarını kullanırken web tabanlı yazılımın güvenlik ayarlarına dikkat ederim.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

24)Şirketimizin bilgisayar ve bilgi güvenliği politikası vardır.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

25)Şirketimizin bilgisayar güvenliği ve bilgi politikasını anlıyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

26)Şirketin bilgisayar güvenliği politikasının dışına çıkıyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

27)İş arkadaşlarımın bilgisayar güvenliği politikasının dışına çıktığını düşünüyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

28)Ben veya iş arkadaşlarım bilgisayar güvenlik politikasına aykırı çalışırsak ve birisi bunu öğrenirse bunun bir yaptırımı olur.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

29)Bir bilgisayar uygulamasında sorun yaşarsam, ağ/sistem yöneticisi veya yardım masası ile iletişime geçmek benim için kolaydır.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

30)Bilgisayar ve bilgi güvenliği üzerine eğitim aldım.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

31)Bilgi güvenliği eğitimi kurumun güvenlik politikasını daha iyi anlamama yardımcı oldu.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

32)Bilgisayar güvenliğine dikkat edersem bilgisayarımı korsanlardan/kimlik avcılardan koruyabileceğimi düşünüyorum*

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

33)Bilgisayar güvenliğine dikkat etmenin önemli olduğunu düşünüyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

34)Bilgisayar güvenliği beni endişelendiriyor.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

35)Bilgisayar güvenliğine özel önem verirsem bunun bir fark yaratacağını düşünüyorum örneğin daha korumalı bir tarayıcı yüklemek gibi.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

36)Bilgisayarımda tuttuğum bilgilerin, insanların bilgisayarıma sızmaya çalışmasını sağlayacak kadar ilgi çekici olmadığını düşünüyorum.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.

37)Bence ne yaparsam yapayım, eğer insanlar kötü niyetliyse bilgisayarıma ve ağımıza girebilirler.

Kesinlikle Katılıyorum
Katılıyorum.
Kararsızım.
Katılmıyorum.
Kesinlikle Katılmıyorum.