T.C.
GÜMÜŞHANE ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

İŞLETME ANABİLİM DALI

TEKNOSTRES'İN BİLGİ GÜVENLİK İHLALİ ETKİSİNDE TEKNO GERİLİMİN ARACI ROLÜ

YÜKSEK LİSANS

Halil İbrahim KAYMAK

OCAK-2023
GÜMÜŞHANE

T.C.
GÜMÜŞHANE ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

İŞLETME ANABİLİM DALI

TEKNOSTRESİN BİLGİ GÜVENLİK İHLALİ ETKİSİNDE TEKNO GERİLİMİN ARACI ROLÜ

THE INTERMEDIATE ROLE OF TECHNO STRAIN IN THE EFFECT OF INFORMATION SECURITY VIOLATION OF TECHNOSTRESS

YÜKSEK LİSANS

Halil İbrahim KAYMAK

OCAK-2023
GÜMÜŞHANE

T.C.
GÜMÜŞHANE ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

İŞLETME ANABİLİM DALI

TEKNOSTRESİN BİLGİ GÜVENLİK İHLALİ ETKİSİNDE TEKNO GERİLİMİN ARACI ROLÜ

THE INTERMEDIATE ROLE OF TECHNO STRAIN IN THE EFFECT OF INFORMATION SECURITY VIOLATION OF TECHNOSTRESS

YÜKSEK LİSANS

Halil İbrahim KAYMAK

Danışman: Doç. Dr. Orkun DEMİRBAĞ

OCAK-2023
GÜMÜŞHANE

BİLİMSEL ETİĞE UYGUNLUK BEYANI

Yüksek Lisans Tezi olarak hazırlamış olduğum "**Teknostresin Bilgi Güvenlik İhlali Etkisinde Tekno Gerilimin Aracı Rolü**" isimli bu tezimin, tamamen kendi çalışmam olduğunu, her alıntıya kaynak gösterdiğimi, alıntı yaptığım tüm çalışmaları kaynakçada belirtiğimi ve Gümüşhane Üniversitesi'nin lisanslı kullanıcısı olduğu intihal yazılım programı ile Lisansüstü Eğitim Enstitüsü'nün belirlediği kıstaslara uygun olarak raporladığımı taahhüt ederim. Tezimin kâğıt ve elektronik kopyalarının Gümüşhane Üniversitesi Lisansüstü Eğitim Enstitüsü arşivinde saklanmasına izin verdiğimi onaylarım.

Lisansüstü Eğitim ve Öğretim Yönetmeliği'nin ilgili maddeleri uyarınca gereğinin yapılmasını arz ederim.

30/01/2023

…….

Halil İbrahim KAYMAK

TEŞEKKÜR

Hazırlamış olduğum “Teknostresin Bilgi Güvenlik İhlali Etkisinde Tekno Gerilimin Aracı Rolü” adlı tez çalışmamda benden güvenini esirgemeyen her zorluk ve her durumda yanımda olan aileme ve arkadaşlarıma desteklerinden dolayı çok teşekkür ediyorum. Akademik yaşantımda bana karşı her zaman anlayışlı ve duyarlı olan, bu tez çalışmasının tamamlanası sürecinde beni her zaman motive edip yanımda olan değerli tez danışmanım Doç. Dr. Orkun DEMİRBAĞ’ a katkıları ve desteklerinden dolayı teşekkürlerimi arz ederim.

Halil İbrahim KAYMAK
GÜMÜŞHANE - 2023

ÖZET

Günümüzde teknoloji çağımıza yön veren en önemli gelişmelerin başında yer almaktadır. Teknolojinin bir getirisi olan bilgi iletişim teknolojilerinde yaşanan gelişimler hızlı bir değişime sebebiyet vermektedir. Bu değişimi takip edebilmek adına çalışanlardan yapabileceklerinden fazlası istenmektedir. Bu durum bilişim alanında faaliyet gösteren bireylerin hata yüzdelerini artırmaktadır. Bu araştırmada bilişim alanı çalışanlarının tekno-stres seviyeleri ile bilgi güvenlik ihlali düzeyleri arasındaki ilişkide tekno-gerilim aracı etkisinin araştırılması amaçlanmıştır. Bu amaç çerçevesinde kolayda örnekleme yöntemiyle Ankara, İstanbul, Kocaeli, İzmir, Trabzon ve Gümüşhane illerinde yaşayan ve bilişim teknolojilerini aktif olarak kullanan 301 katılımcıdan araştırma verileri elde edilmiştir. Araştırmadan elde edilen sonuçlar yüksek tekno-stres düzeyinin tekno-gerilim ile pozitif ilişkili olduğunu göstermektedir. Bunun yanında yüksek tekno-stres düzeyinin bilgi güvenlik politikası ihlali ile pozitif ilişkili olduğu araştırmanın bir diğer bulgusudur. Bu bulgulara ek olarak tekno-gerilim düzeyinin bilgi güvenlik politikası ihlali ile pozitif ilişkili olduğu ortaya konulmuştur. Araştırmanın son bulgusu olarak tekno-gerilim düzeyinin tekno-stresle bilgi güvenliği ihlali arasında aracı etkisinin olduğu sonucuna ulaşılmıştır. Bu sonuçlardan hareketle çalışanların tekno-stres ve tekno-gerilim düzeylerini azaltacak organizasyonlar yapılması önerilmektedir. Buna ek olarak bilgi güvenliği ihlalleri noktasında politikaların geliştirilmesi ve uygulanması bir diğer öneri olarak yer almaktadır.

Anahtar Kelimeler: Bilgi güvenliği politikası ihlali, Tekno-gerilim, Tekno-stres

SUMMARY

Technology is currently at the summit of the list of crucial advancements that shape our time. A rapid shift is brought on by the advancements in information and communication technologies, which are a return to technology. This shift must be adhered to by more than just employees. As a result, more people working in the technology industry make mistakes. The purpose of this study is to look into the connection between workers working in the information field and levels of technological stress and information security breaches. Using the simple sampling technique, study data were gathered from 301 participants who resided in the provinces of Ankara, Istanbul, Kocaeli, Izmir, Trabzon, and Gümüşhane and actively used information technologies. The study's findings demonstrate a positive correlation between elevated levels of techno-stress and techno-strain. In addition, information security policy violations are favorably correlated with high levels of techno-stress. In addition to these results, it has been established that the infringement of the information security policy and the techno-strain level are favorably correlated. The most recent study finding was that there is a mediating relationship between information security violation and techno-strain level. It is advised that organizations decrease employee levels of technological stress and tension in light of these findings. Another suggestion is the creation and application of policies at the place where information security is violated.

Keywords: Information security policy violation, Techno-strain, Techno-stress

İÇİNDEKİLER

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

EKLER DİZİNİ

SİMGELER VE KISALTMALAR DİZİNİ

AVE	: Ortalama Açıklanan Varyans
BGI	: Bilgi güvenliği ihlali
BGPI	: Bilgi güvenliği politikası ihlali
CFI	: Karşılaştırmalı uyum indeksi
CI	: Önyükleme güven aralığı
CR	: Bileşik güvenirlik değeri
DFA	: Doğrulayıcı faktör analizi
DT	: Tekno-belirsizlik
GDT	: Genel caydırıcılık teorisi
GFI	: Uyum iyiliği indeksi
PMT	: Koruma motivasyon teorisi
RMSEA	: Kestirim hatalarının ortalama karekökü
SEN	: Bilgi güvenlik politikası ihlali
SRMR	: Hata kareler ortalaması karekökü
TAY	: Tekno iş yükü
TG	: Tekno-gerilim
TGK	: Tekno-güvensizlik
TI	: Tekno-istila
TK	: Tekno-karmaşıklık
TLI	: Normlandırılmamış uyum endeksi
TST	: Teknostres
VIF	: Varyans genişletme faktörü

1. GİRİŞ

Bilgi ve teknoloji çağı olarak adlandırılan 21. yüzyıl gerek bireysel hayatımızı gerekse de profesyonelce yürütmemiz gereken yaşantılarımızı dijital mecralara taşıyarak daha gelişmiş, yenilikçi fakat aynı zamanda daha karmaşık hale getirmiştir (Shadbad ve Biros, 2020). Bu yenilikçi dijital mecralar arasından bulut bilişim sistemleri, yapay zekâ ve nesnelerin interneti gibi teknolojiler profesyonel iş ortamlarına uyarlandıkları için önemli değişikliklere neden olmuşlardır (Forman vd., 2014; Şimşek-Demirbağ ve Yıldırım, 2021). Bu yeni teknolojik sistemler iş yerlerine etkinlik, verimlilik ve performans noktasında pozitif katkılar sunsa da bilgi güvenlik ihlali gibi başlıca konularda negatif etkiler bırakabilmektedirler (Atanasoff ve Venable, 2017). Çağımızda bilgi ve iletişim teknolojilerini kullanan örgütler özellikle bilgi sistemlerine ciddi yatırımlar yapmaktadırlar. Örgütler yaptıkları yatırımlarla buradan doğabilecek ihlallerden kaynaklı riskleri en aza indirmeye çalışmaktadırlar. Örneğin örgütlerin işleyişi gereği karşılaşabilecekleri bilgi güvenliğinden kaynaklanan riskler, kurumsal sorumluluklar, örgütün yaşayabileceği güven kaybı ve maddi zararlar önemli olumsuzluklara sebebiyet verebilir (Cavusoglu vd., 2004). Buradan hareketle örgütün bilgi güvenliğini sağlamak en öncelikli alanlardan birini oluşturmaktadır (Ransbotham ve Mitra, 2009). Nitekim gelinen son 10 yılda birçok firmanın yaşamış olduğu bilgi güvenliğinden kaynaklı ihlaller, örgütler için bilgi güvenliğinin ne kadar önemli ve acil bir olgu olduğunu ortaya koymaktadır (Chen vd., 2018). Citibank, Facebook, JPmorgan, Nestle ve Target gibi birçok önemli şirket yaşamış oldukları bilgi güvenlik ihlalleri nedeniyle oluşan açığı kapatabilmek için milyarlarca dolar harcamak zorunda kalmışlardır. Aslında bu şirketlerde yaşanan veri ihlalleri yalnızca yazılım ve donanım sistemlerini içeren önlemlerin yetersizliğinden kaynaklanmamaktadır. Örneğin bu şirketler arasında bulunan Target'taki veri güvenliğinden kaynaklı ihlal, şirkete ait bilgilerin spam bir e-posta gönderileri aracılığıyla birlikte çalıştığı ortağınca illegal bir şekilde elde edilmesi sonucu meydana gelmiştir (Chen vd., 2018). Buradan hareketle alınabilecek güvenlik önlemlerindeki en zayıf halkanın "insandan kaynaklı etkenler" olduğu söylenebilir. 2017'de Singapur'da yapılan "The Global State of Information Security Survey" isimli araştırmanın sonuç rapurunda şirketlerin uğradığı siber saldırıların %38'inin kurumda aktif olarak çalışan personelin yapmış olduğu hatalardan kaynaklandığı tespit edilmiştir. Yine Lewis (2003) tarafından yapılan bir başka araştırmada ekonomik olarak zararla neticelenen bilgi güvenliği ihlallerinin %65'inin

çalışanların sebep olduğu hatalardan kaynaklandığı tespit edilmiştir. Benzer bir araştırmada Klahr vd. (2017) şirketlere yapılan siber saldırıların tamamen dış kaynaklı olmadığı, örgüt çalışanlarının yapmış oldukları hataların da önemli açıklara sebep olduğu belirtilmiştir. Bunun yanında güncel ve güvenilir olmayan virüs programları kullanılmasının veya örgüt elemanlarının siber güvenlik konularında bilgi eksikliklerinin olmasının önemli açıklara sebep olduğu araştırmanın dikkate değer bir diğer sonucu olarak karşımıza çıkmaktadır. İnsandan kaynaklanan hatalar, teknik olarak ortaya çıkabilecek hatalara kıyasla daha önemli bilgi güvenliği ihlalleri ortaya çıkarabilmektedir (Ahmed vd., 2012). Bilgi güvenlik ihlalini de içine alan genel anlamda ihlal, yapılan çalışmalarda (Ragu-Nathan vd., 2008; Tarafdar vd., 2007; Wang vd., 2008) tekno-stresin sebebi olarak karşımıza çıkmaktadır. TST kavramı Tarafdar vd. (2010) tarafından bilgi ve iletişim teknolojilerini kullanan kişilerin sürekli olarak teknolojiyi takipte olmaları, çok fazla bilgi yüklenmeleri, sürekli olarak yapılan sistem güncellemeleriyle yeniliklere ayak uyduramamaları gibi nedenlerle yaşamış oldukları stres durumu olarak ifade edilmiştir. Bu stres durumu kişilerde düş kırıklığı, zorlanma, üst seviye kaygı, kafa karışıklıkları gibi bir takım negatif duygular oluşturabilmektedir (Weil ve Rosen, 1997). Bu negatif duygular nedeniyle iş yerinde stres oluşturabilen teknoloji kaynaklı faktörler çalışanların daha fazla stres yaşamalarına sebep olmaktadır (Türen vd., 2015). Örgüt çalışanlarının daha fazla stres yaşamaları buna paralel olarak daha fazla teknolojik gerilim yaşamalarına etki edebilir. Örneğin Ayyagari vd. (2011) yaptıkları araştırmada çalışanların iş ortamında daha fazla stres yaşamalarının teknolojik gerilimlerini de artırdığını belirlemişlerdir. Yanlızca stres düzeyiyle ilişkili olmayan teknolojik gerilimin birçok değişkene etki edebildiği alanyazında görülmektedir (Fuglseth ve Sørebø, 2014; Sareen, 2019; Turel ve Gaudioso, 2018). Nitekim örgüt çalışanlarının teknolojinin sebeb olduğu gerilim nedeniyle yaşabilecekleri bir baskı onları daha fazla hata yapmaya zorlayabilir. Bunun bir sonucu olarak çalışanlar bilgi güvenliği noktasında ihlallere sebep olabilirler (Shadbad ve Biros, 2020). İlgili alanyazına bakıldığında TST, TG ve BGI değişkenlerinin birlikte nasıl bir etki oluşturduklarına yönelik araştırmaların oldukça sınırlı olduğu görülmektedir (Shadbad ve Biros, 2020). Özellikle bilişim sektöründe sıklıkla karşılaşılabilen tekno-stresin tekno-gerilim ve bilgi güvenliği ihlallerinden ne düzeyde etkilendiği belirlemek önem arz etmektedir. Buradan hareketle yapılan araştırmada tekno-stres ile bilgi güvenliği arasındaki ilişkide tekno-gerilimin aracılık etkisinin test edilmesi amaçlanmaktadır. Ortaya konulacak bu değerlendirmenin örgütlere gerekli önlemleri alabilmeleri ve verimliliği artırabilmeleri noktasında önemli katkılar sunacağı düşünülmektedir.

2. LİTERATÜR TARAMASI VE KAVRAMSAL ÇERÇEVE

2.1. Tekno-Stres

Günümüz dünyasında teknolojik gelişmeler ve bunların günlük hayatta kullanımı önemli bir yer tutmaktadır. Özellikle bilgi ve iletişim teknolojilerinde ortaya çıkan gelişmeler çalışma ortamlarında da bir takım değişimleri beraberinde getirmektedir. Teknoloji her ne kadar iş yerlerinde üretkenlik, verimlilik, kurum içi gelişmiş bir iletişim ağı gibi olumlu getiriler sağlasa da işverenler ve çalışanlar için teknoloji kullanımından kaynaklı bazı olumsuz sonuçlar doğabilmektedir (Boyer-Davis, 2018). Bu olumsuz sonuçlardan biri de tekno-stres olarak adlandırılan kavram ile karşımıza çıkmaktadır.

İlk kez Dr. Craig Brod tarafından ortaya atılan tekno-stres kavramı "ortaya çıkan yeni bilgisayar teknolojileriyle baş edememe sonucu meydana gelen modern bir uyum hastalığı" olarak ifade edilmiştir (Brod, 1984). Bu tanım her ne kadar tekno-stresi bir hastalık olarak sınıflandırsa da bazı araştırmacılar bu durumu teknolojinin getirmiş olduğu uyumsuzluk olarak ifade etmiştir (Doğrular, 2019). Bu kavrama başka bir açıklama getiren Weil ve Rosen (1997) ise tekno-stresi "kişide meydana gelen stres kaynaklı etmenlerin (endişe, korku, öfke vb.) teknoloji nedeniyle ortaya çıkması" olarak tanımlamıştır. Tekno-stres ile ilgili yapılan tanımlamalar incelendiğinde ortak vurgunun teknolojilerde meydana gelen değişimler ve bu değişimlerin örgüt çalışanları üzerindeki etkileri olduğu görülmektedir (İlseven, 2019). Bu noktada yapılan tanımlamalarda her ne kadar teknoloji kaynaklı zihinsel stres vurgulansa da tekno-stres kavramı aşırı düzeyde fiziksel ve duygusal uyarılmayı da kapsamaktadır (Atanasoff, 2017). Bütün bu tetikleyicilerin bir araya gelmesi ise kişinin yeniliklere uyum sağlayamama, değişime karşı direnç gösterme, işinden memnun olmama, işten ayrılma ya da devamsızlık gösterme gibi sonuçları beraberinde getirmektedir (Torres, 2021). Nitekim yönetilemeyen bu stresin işyerindeki yansımalarına bakıldığında daha fazla endişe, mental olarak yorgunluk, şüphecilik ve verimsizlik sıklıkla karşımıza çıkmaktadır (Salanova vd., 2007). Bu durumun doğal bir sonucu olarak da bireysel ve örgütsel verimlilik olumsuz etkilenmektedir (Tarafdar vd., 2007).

Örgütlerin son 30 yıldaki gelişimleri dikkate alındığında özellikle mobil telefonlar, internet, otomatik kontrol sistemleri, bilgisayar ve yapay zekâ gibi alanlarda hızlı değişimler kat ettikleri görülmektedir. Bu ekipmanlar her ne kadar örgütteki

işleyişi kolaylaştırsa da uzaktan denetim mekanizması, birçok alanda yapılan görevlendirmeler, sosyal izolasyon ve işten soyutlanma sorunsallarını da beraberinde getirmektedir (Ragu-Nathan vd., 2008). Ayrıca bu teknolojik yenilikler sonucunda çalışma şartları değişen çalışanların da yeni koşullara mecburen uyum sağlamak zorunda kaldıkları bir gerçektir (Brand, 2000). Yine gelişen teknolojiler nedeniyle alınması gereken eğitimlerin eksikliği, iş yöntemlerinde değişimlerin ortaya çıkması çalışanlarda teknolojik uyum eksikliğini ortaya çıkarmaktadır (Yener, 2018). Tüm bu durumlar da çalışanlarda daha fazla tekno-stres sorunu ile sonuçlanmaktadır. Yaşanan aşırı tekno-stresin getirmiş olduğu kaygının nihai bir sonucu olarak da ağırlıklı olarak teknolojiye dayalı sektörlerde çalışan bireylerde daha fazla somatik ve psikosomatik bozukluklar ortaya çıkmaktadır (Boyer-Davis, 2018). Nitekim stres alanında önemli çalışmaları bulunan Lazarus (1984), stresin bilişsel, duygusal, fizyolojik, psikolojik ve nörolojik olarak çok boyutlu alanlarda bütüncül bir etkisinin olduğunu ortaya koymaktadır. Stresin birey üzerindeki etkilerine bakıldığında yorgunluk, baş ağrısı, dingin olamama ve aşırı öfkeli olma gibi birçok olumsuz sonucu bünyesinde barındırdığı görülmektedir (Arnetz ve Wilholm, 1997). Strese daha farklı bir perspektiften bakan Clark ve Kalin (1996)'a göre bireyde ortaya çıkan stres teknolojinin doğal bir sonucu olarak meydana gelmektedir. Oldukça doğal olarak ortaya çıkan stres duygusunda teknolojik gelişimler aslında bir suçlu değil araç olarak görülmelidir. Araştırmacılara göre tekno-stresi yönetebilmek için teknolojiyi yönetme çabasından ziyade değişimin kendisini yönetme üzerine odaklanılmalıdır.

Tekno-stres, alanyazında ağırlıklı olarak olumsuz bir faktör olarak karşımıza çıksa da Salo vd. (2018) tekno-stres açısından yaşanan negatif duyguların kötü strese, pozitif duyguların ise iyi strese neden olduğunu belirtmişlerdir. Bu bağlamda kötü stres ile kastedilen daha çok çalışanların bilgi teknolojilerini bir tehdit olarak görmeleri sonucu yaşamış oldukları olumsuz duygulanım halidir (Tarafdar vd., 2019). Tekno-stresi ortaya çıkaran belirleyicilere bakıldığında tekno-istila, tekno-belirsizlik, tekno-karmaşıklık, tekno-güvensizlik ve tekno-iş yükü boyutlarının çalışanların hayatında olumsuz etkiler bıraktığı görülmektedir (Tarafdar vd., 2007). Nitekim bu durumun çalışanların aynı zamanda iş hayatlarında da olumsuz etkiler meydana getirebildiği söylenebilir (Yener, 2018).

2.1.1. Tekno-Stres Boyutları

Tekno-stresin boyutlarıyla ilgili alanyazın incelendiğinde Tarafdar vd. (2007)'de yaptıkları çalışma karşımıza çıkmaktadır. Buna göre tekno-stres tekno-aşırı yük (TAY),

tekno-karmaşıklık (TK), tekno-belirsizlik (TB), tekno-istila (TI) ve tekno-güvensizlik (TGK) olmak üzere beş boyutta açıklanmıştır. Bu beş boyuttan ilki tekno-aşırı yük olarak ifade edilmiştir.

2.1.1.1. Tekno-Aşırı Yük

Bilgi iletişim sistemlerini ve bilişim teknolojilerini kullanan örgüt çalışanlarının çok daha hızlı ve uzun süreli çalışmaya zorlandıkları durumlar tekno-aşırı yük kavramı ile ifade edilir (Tarafdar vd., 2007). Çalışanlar teknolojik gelişmelerin getirdiği çok sayıda bilgi ve teknolojik aygıtın eş güdümlü olarak kullanımı sayesinde daha az bir zamanda çok daha fazla iş yapabilme olanağına kavuşmuşlardır (İlseven, 2019). Ancak bu durum yoğun bilgi akışı nedeniyle bir süre sonra çalışanlarda yorgunluk oluşmasına sebep olmuştur (Tarafdar vd., 2007). Nitekim Lehto ve Landry (2012) aşırı düzeyde gerçekleştirilen hızlı işlem yükünün örgüt çalışanları üzerinde bir takım bilgi taşmalarına ve aşırı yüklemelere neden olabileceğini belirtmişlerdir. Böyle bir durumda çalışanlar daha hızlı iş yapmak için teşvik edilmekte beraber bu sorumluluk sonucu hata yapma olasılıklarında artışlar olabilecektir. Bu nedenle ortaya çıkabilecek olumsuz sonuçlar ise çalışanların stres düzeylerini yükseltecektir (Türen vd., 2015).

Örgüt çalışanlarının aşırı bilgi yüklemesi ile karşı karşıya kalmaları verimli olarak kullanabileceklerinden daha çok bilgiyi edinmelerine sebep olacaktır. Katılımcıların eş zamanlı gelen e-posta ve sistemsel uyarılara en kısa zamanda katılmaya mecbur bırakılmaları bu duruma örnek olarak verilebilir. Böyle bir durumla karşı karşıya kalan iş yeri çalışanları ise endişe ve gerilim duyguları yaşayarak dikkat dağınıklığı sorunuyla yüz yüze kalabilecektir (Tarafdar vd., 2011). Eppler ve Mengis (2004)'e göre kişisel faktörler, bilginin özellikleri, görev ya da sürecin parametreleri, organizasyonel tasarım ve bilgi teknolojisi olmak üzere beş faktörün bir araya gelmesiyle aşırı bilgi yükü oluşur. Belirtilen bu faktörler örgüt çalışanının süreç içerisindeki bilgi işleme kapasitesini etkiler. Nitekim tekno-aşırı yüke maruz kalan çalışanların kişisel sağlık, işten ayrılma düşüncesi ve mesleki tatmin tehditleri ile karşılaşabilecekleri bilinmektedir (Tarafdar vd., 2007).

2.1.1.2. Tekno-İstila

Tekno-istila, bilgi ve iletişim teknolojileri temelli çalışanların yoğun teknoloji kullanımları nedeniyle sürekli ulaşılabilir olmaları ve bunun sonucunda iş ile yaşamında denge kuramamalarını ifade etmektedir (Tarafdar vd., 2007). Nitekim bu kişiler sürekli çevrimiçi oldukları için zorunlu olarak aile hayatlarını ve sosyal yaşamlarını da işlerinin

bir parçası haline getirebilmektedirler. Gerek internet gibi ağlar gerekse de mobil olarak işlem görebilen kablosuz bilgi işlem cihazları (akıllı telefonlar, tabletler vb.) bireylerin her yerde ve sürekli olarak çevrimiçi olmaya izin verir (Clark ve Kalin, 1996). Bu nedenle böyle bir duruma maruz kalan örgüt çalışanları sürekli çevrimiçi oldukları için gergin bir ruh hali içerisindedirler. (Tarabah, 2021). Teknolojinin çalışanlar üzerinde ortaya çıkarmış olduğu bu durum ise bireylerin kişisel hayatını ya da aile yaşamını ihmal etmesine ve daha az vakit geçirmesine sebep olmaktadır (Wang vd., 2008).

Örgüt çalışanlarının sürekli çevrimiçi olma gerekliliği, kişilerin bu teknolojilere bağlı olarak yaşamalarına sebep olmaktadır. Teknolojinin çalışanların hayatlarına istemeden ve kişisel rızaları olmadan bu düzeyde dâhil olması onlarda gerginlik ve stres oluşturabilmektedir (Tarafdar vd., 2011). Örgüt çalışanlarının işleri gereği yapmaları gereken görevlerle kişisel yaşantılarının iç içe geçmesi strese sebep olan bir diğer etmen olarak görülebilir (İlseven, 2019). Bütün bu durumlar bireyin aile ve sosyal yaşantısına yeterince vakit ayıramamasına ve gerek iş yerinde gerekse de aile ortamında çatışmalar yaşamasına sebep olmaktadır (Merdan, 2021).

2.1.1.3. Tekno-Karmaşıklık

Tekno-karmaşıklık, örgüt çalışanlarının hızlı bir şekilde ve sürekli olarak gelişen teknolojiyi, ortaya çıkan yeni donanım ve yazılım sistemlerini gerek anlama gerekse de uygulama noktasında kendini yetersiz görmesi durumunda çok daha fazla zaman ve gayret sarf etmesi sonucu yaşamış olduğu stres olarak tanımlanır (Tarafdar vd., 2007). Böyle bir durumda örgüt çalışanlarının teknolojik karmaşıklıktan daha az etkilenmeleri için olması gerekenden çok daha fazla çalışmaları zorunludur. Bu yeni ve karmaşık teknolojileri öğrenerek çağa ayak uydurmak zorunda kalan örgüt çalışanlarının bu uygulamaları öğrenmeleri çok daha uzun vakitler alabildiği için kendilerinde strese yol açabilmektedir (İlseven, 2019). Nitekim bireylerin sürekli olarak güncellenen yeni yazılım, donanım ve bunlara ait uygulamaları öğrenmeleri yeni teknik bilgiler ve yöntemler gerektirdiği için karmaşık görünebilir. Bu durumda örgüt çalışanlarının bu yeni uygulamaları öğrenmeleri haftalarca sürebilir. Bunun bir sonucu olarak da çalışanlar çok daha fazla zaman ve çaba harcayabilirler. Bu iş için harcanan daha fazla zaman ve emek çalışanların yeni kuralları öğrenirken anlaşılmasının zor olduğu durumlarda kişisel eleştiriler ve yetersizlik algısı meydana getirebilir. Böyle bir durum yine çalışanların stres yaşamalarına sebep olabilecektir (Kopuz ve Aydınlı, 2020). Bunun yanında yeni teknolojilerin iş ortamına kazandırılması noktasında çok hızlı hareket edilmesi de çalışanlarda stres oluşturan bir diğer etmen olarak karşımıza

çıkmaktadır (Türen vd., 2015). Belirtilen bütün bu faktörler çalışanların güncellenen teknolojiye ayak uydurabilmek için daha fazla zaman ve çaba harcamalarını zorunlu hale getirdiğinde tekno-karmaşıklık ortaya çıkar (Chandra vd., 2015).

2.1.1.4. Tekno-Güvensizlik

Günümüz dünyasında hemen hemen her birey teknolojide meydana gelen hızlı değişimlere ayak uydurmakta zorlanmaktadır. Özellikle teknolojiyi kullanma noktasında zorluk yaşamayan bireylere göre teknoloji kullanımında daha fazla güçlük yaşayan bireyler bu rahatsızlığı daha fazla hissetmektedir (Çalışkan, 2022). Tekno-güvensizlik, örgüt çalışanlarının devamlı olarak gelişim kaydeden bilgi ve iletişim teknolojileri sebebiyle sahip oldukları işlerini kaybetmekten korkmalarını ve bu durum nedeniyle birbirlerine olan güvensizlik durumlarını ifade etmektedir (Tarafdar vd., 2007). Califf vd. (2020) tekno-güvensizliği "bilgi ve iletişim teknolojilerini kullanan çalışanların, bu sistemleri kullanan diğer çalışanlara göre kendilerini daha donanımsız ve bilgisiz oldukları yönünde algılamaları neticesinde ortaya çıkan durum" olarak tanımlamıştır. Böyle bir durumda örgüt çalışanları teknolojiye ve değişime ayak uyduramadıklarını düşünecekleri için işlerini kaybetme korkusuyla stres yaşayabilecekleridir (İlseven, 2019). Çalışanların yaşamış oldukları bu korku duygusunu tekno-güvensizlik kavramı karşılamaktadır (Wang vd., 2008). İş yeri çalışanlarının yaşamış oldukları bu korku duygusunun bir diğer olumsuz sonucu da kendilerine güvensizlik olarak karşımıza çıkmaktadır (Tarafdar vd., 2011).

2.1.1.5. Tekno-Belirsizlik

Bilgi-iletişim teknolojilerini içerisinde barındıran yazılım ve donanım sistemlerinde meydana gelen ve süreklilik arz eden değişimler çalışanlarda bir süre sonra rahatsızlık hissi oluşturmaktadır (Wang vd., 2008). Bu çerçevede sürekli olarak değişen ve bir sonraki adımında nasıl bir güncelleme ile karşılaşabileceği noktasında önünü göremeyen çalışanların yaşamış olduğu durum tekno-belirsizlik kavramı ile ifade edilmektedir (Yener, 2018). Bu durum çalışanların yüksek düzeyde tedirginlik ve kararsızlık duyguları yaşamalarına sebep olmaktadır (Park ve Cho, 2016). Nitekim teknolojinin sürekli değişmesiyle birlikte örgüt çalışanları deneyim sahibi oldukları alanlarda uzmanlaşamadan diğer güncellemeyle yüz yüze kalmaktadırlar. Bunun bir sonucu olarak çalışanlar bu değişime ayak uyduramadıklarını düşünebileceklerinden hayal kırıklığı ve stres yaşayabilirler (Tarafdar vd., 2011). Örgüt çalışanları başlangıçta teknolojideki yeni gelişmeler ve değişimler hakkında hevesli olsalar da bu yenilikleri

öğrenemediklerini ya da bunlara ayak uyduramadıklarını düşündüklerinde endişe ve tedirginlik duygularıyla yüzleşebilirler (Çetin ve Bülbül, 2017).

2.2. Tekno-Stresin Nedenleri, Belirtileri ve Öncüleri

Tekno-strese neden olan faktörlerin belirlenmesi noktasında alanyazında birçok araştırma bulunmaktadır. Bu çalışmalar içerisinde Ragu-Nathan vd. (2008)'de yaptıkları çalışma dikkate değerdir. Araştırmacılara göre bilgi-iletişim teknolojilerinin genel anlamda karmaşık bir yapı göstermesi, bu teknolojilerde meydana gelen hızlı değişimler sonucu çalışanların ayak uyduramaması, sürekli çalışma gerektirmesi ve bu durumun iş görenlere aşırı bir yük getirmesi, yaşanabilecek teknik aksaklıklarla mücadele edilememesinin getireceği endişe tekno-strese neden olmaktadır. Tekno-stresin nedenleri üzerine araştırmalar yapan bir başka çalışmacı Brod (1984) teknoloji kullanımına ilişkin kişisel deneyim, yaş faktörü, denetim mekanizmasının baskılayıcı etkisi ve iş yeri ortamının etkisi gibi etmenlerin teknos-stresin muhtemel sebepleri arasında bulunduklarını ifade etmiştir. Champion (1988) tekno-stresi çevresel ve sosyal olarak iki aşamada incelemiştir. Çevresel tekno-stres etmenleri altında uygunsuz iş yeri ortamı, yeterli olmayan güvenlik hizmeti, yetersiz donanım ve yazılım sistemleri, deneyimli personel eksikliği ve finansman yetersizliği sıralanabilir. Sosyal etmenler arasında ise çalışma ortamındaki teknoloji kaynaklı menfaateler, makam kavgaları, görev yerlerindeki değişiklikler, istihdam sorunları ve hiyerarşi kaynaklı sorunlar yer almaktadır. Tekno-stresin nedenlerini daha genel bir çatı altında toplamaya çalışan Çoklar vd. (2016) ise bireysel, eğitimsel, sağlık sorunları temelli, zamandan ve teknik sebeplerden kaynaklı olmak üzere çeşitli başlıklar altında bu etmenleri toplamışlardır.

2.3. Tekno-Stresi Önleme ve Başa Çıkma Yolları

İş yerlerinde yoğun teknoloji kullanımının beraberinde getirdiği sorunlar ve bu sorunlarla nasıl baş edilebileceği önemli bir çalışma alanını oluşturmaktadır. Nitekim bu geçiş süreçlerinde örgüt çalışanları bir takım davranışlar gösterebilmektedirler. Rodoplu (2008)'ya göre teknolojik değişimler nedeniyle yeni alışkanlıklara geçiş sürecinde çalışanlar kabullenmeme/kabul etme, reddetme, direniş, uyumlama, destek olma ve kabullenme davranışları göstermektedirler. Selye'nin stres karşısındaki "genel adaptasyon sendromu" aşamalarına oldukça benzerlik gösteren bu modelleme (Peterson, 1999) tekno-stresle başa çıkma noktasında bireyde meydana gelen aşamaları kapsamlı olarak ortaya koymaktadır.

Tekno-stresin temel boyutları arasında bulunan tekno-aşırı yük, tekno-istila, tekno-karmaşıklık, tekno-belirsizlik ve tekno-güvensizlik etmenlerinin oluşturduğu etkiyi en aza indirgemek için iş yeri bazında önlemler alınmalıdır (Pirkkalainen vd., 2019). Bu önlemler arasında örgüt çalışanlarına teknik destek sağlama, teknolojik okur-yazarlığın arttırılması çalışmaları, teknolojiye katılımın kolaylaştırılması ve yenilikler noktasında destekleyici tutumlar önemli bir yer tutmaktadır (Tarafdar vd., 2011). Yine tekno-stres ile baş etme yolları arasında kullanıcıların basitçe uygulayabilecekleri yazılımlar tercih edilmesi, teknolojilerin kolaylıkla uygulanabileceği güvenli ortamlar oluşturulması, güncellenen teknolojilerle ilgili çalışanların eğitilmesi oldukça önemlidir (Walinga, 2014). Bütün bu baş etme yollarına ek olarak Ragu-Nathan vd. (2008) bir takım stratejiler önermişlerdir. Bu stratejiler aşağıda sıralanmıştır;

- Tekno-stresin olumsuz etkilerini azaltma adına çalışanların stres yönetimini sağlamak
- Çalışanların rahatlama tekniklerini kullanması
- Kas gevşetme egzersizleri
- Yemek düzeninin ve seçiminin iyileştirilmesi
- Çalışma saatlerine ilişkin mola zamanı aralıklarının düzenlenmesi
- Müzik dinlemek
- Rahatlama ve zaman yönetimi kavramlarının hayatın her alanına uygulanması
- Ekip çalışmaları ve teknoloji olmadan vakit geçirmek
- Tekno-strese ilişkin farkındalık oluşturmak
- Sağlık ve dengeli bir iş hayatı oluşturmak

2.4. Tekno-Gerilim

Lee ve Ashforth (1996) gerginliği, kişinin enerji eksikliği hissetmesi ve stresli olaylarla başa çıkmak için hiçbir duygusal kaynağa sahip olmaması olarak tanımlamıştır. Bu gerilime teknolojinin dâhil olmasıyla oluşan teknolojik gerginliği ise Salanova vd. (2014) başa çıkamamanın neden olduğu kaygı, zihinsel tükenme, şüphecilik ve etkisizlik olarak ifade etmişlerdir. Tekno gerginlik, aynı zamanda bireyin strese tepki olarak gösterdiği olumsuz durum olarak da nitelendirilebilir (Jackson ve Schuler, 1985). Nisafani vd. (2020) teknolojik gerilimi teknostresi açıklayan önemli bir değişken olarak tanımlamaktadırlar. Tanımlanan bu kavramsal modelle tekno-belirsizliğin, tekno-karmaşıklığın ve teknoloji bağımlılığının teknostresin bazı nedenleri olduğu ortaya konulmuştur. Belirtilen bu nedenlerin yanında çalışanlarda duygusal tükenme ile öfke ve kaygı gibi bazı olumsuz duygular içeren gerginliklerin oluştuğu

tespit edilmiştir (Nisafani vd., 2020). Araştırmacılar strese neden olan durumların gerginliğe yol açtığını ve bu gerginliğin örgütsel sonuçları etkilediğini öne sürmüşlerdir (Cooper vd., 2002). Buna ek olarak Galluch vd. (2015) stresin çeşitlerinden olan teknostresin de iş tatmini, üretkenlik, BİT kullanımı ve tükenmişlik gibi örgütsel sonuçları etkileyen hem fizyolojik hem de psikolojik gerginliğe sebep olduğunu çalışmalarında belirtmişlerdir (Galluch vd., 2015). Bununla birlikte Ayyagari vd. (2011) teknostres tiplerinin daha yüksek bir gerilim seviyesine yol açacağını öne sürmüşlerdir. Yapılan çalışmalar dikkate alındığında teknostresle birlikte tekno gerilimin ortaya çıktığı düşünülebilir (Brown vd., 2014; Fieseler vd., 2014; Fuglseth ve Sørebø, 2014; Shadbad vd., 2020).

2.4.1. İşe Bağlı Gerilim

İşe bağlı stres ve gerginlik genellikle aynı ifade olarak kullanılmaktadır. Fakat stres biyolojik, psikolojik ya da sosyal bir sistemde dışsal bir yükün ya da talebin olması iken gerginlik stresin sistemde oluşturduğu bozulma olarak tanımlanmaktadır (Lazarus, 1984). Piko (1999)'ya göre işe bağlı gerginlik yapılan işin, çalışanın ve örgütün yaşadıkları olumsuz sonuçlardır. Bir başka deyişle işe bağlı gerginlik çalışandan beklenilen ile çalışanların bu beklentileri yerine getirmesi arasındaki ilişkinin sonucudur (Karasek, 1979). Saganuwan vd. (2015)'ye göre bireylerin iş yeri teknolojisi özelliklerine ilişkin algıları olumsuzsa kişi ve çevre arasında bir uyumsuzluk meydana gelir. Bu uyumsuzluk sonucu oluşan durum iş sonuçlarını olumsuz yönde etkiler. Sonuç olarak da gerginlikte bir artışa sebep olur (Saganuwan vd., 2015).

2.4.2. Tekno-Gerilimi Önleme ve Başa Çıkma Yolları

Stresi meydana getiren temel kaynaklardan gerilime kadar olan süreçte örgütsel teknoloji eğitim programları, iç iletişim ve kişilik özellikleri gibi düzenleyici faktörler teknostres ile örgütsel sonuçlar arasındaki ilişkiyi düzenleyebilmektedir (Pirkkalainen vd., 2019; Tarafdar vd., 2015; Zainun vd., 2019). Buna ek olarak, örgütsel mekanizmalar ya da bireylerin stresle başa çıkma yetenekleri gibi durumsal faktörlerin stres etkeni ile gerilim ilişkisini yumuşattığı ve gerilimin örgütsel sonuçlar üzerinde etkilerini azalttığı görülmüştür. (Lazarus ve Folkman, 1984) İşe bağlı gerginlikle başa çıkmada yapılacak bireysel yöntemlere örnek olarak olumlu düşünmek, spor yapmak, eğlenmek, kişinin iş arkadaşlarıyla arkadaşlık kurabilmesi, hobiler edinmek, seyahate çıkmak, kişinin davranışlarını kendi kontrolü altında tutabilmesi gibi yöntemler önerilebilmektedir (Erdoğan vd., 2009). Başa çıkma yollarını örgüt düzeyinde ele

alırsak örgütün stres kaynaklarını araştırması ve buna yönelik çözümler bulması gerekmektedir (Kopuz, 2013).

2.5. Bilgi Güvenliği İhlali

Türk Dil Kurumu (2012) bilgiyi insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü olarak tanımlamaktadır. Bilginin günümüzde en çok kullanıldığı alan bilişim sistemleridir (Çek, 2017). Bilişim sistemleri aracılığıyla bilgi ulaşılabilir hale gelerek kurumsal sorunlara çözümler için kullanılabilmektedir. (Özer, 2011). Bilginin içeriğinin değiştirilmeden ve istenmeyen kişiler tarafından elde edilmeden, gizlilik içerisinde göndericiden alıcısına aktarılmasına bilgi güvenliği denir (Pfleeger, 1997). Uluslararası standart olarak bilinen ISO / IEC 27002, bilgi güvenliğini bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması olarak da ifade etmektedir (Tekerek, 2008). Gizlilik kavramı bilginin sadece istenilen kişiler tarafından elde edilmesi, bütünlük bilginin değişikliye uğramaması ve eksiksiz olması, kullanılabilirlik ise bilginin her an ulaşılabilir halde olması şeklinde tanımlanabilir (Fussel, 2005).

Günümüz koşullarında bilgi güvenliği çeşitli sebeplerle çalışanlar tarafından ihlallere uğramaktadır. Bilgi güvenliği ihlali, var olan bilgi güvenliği politikalarının ve kontrollerinin başarısız olması durumu veya güvenlikle ilgili önceden bilinemeyen, hizmet ve ağ sistemlerindeki aksaklıkların bütünü olarak tanımlanabilir (Akay, 2014). Kuruluşlar, siber sapkınlar tarafından gerçekleştirilen dış saldırılarla aşırı derecede ilgilenirken, araştırmacılar, şirket içindeki kişiler tarafından gerçekleştirilen ihlallerin, kuruluşların bilgi varlıkları için daha da büyük bir tehlike ve zarar oluşturduğunu iddia etmiştir (D'Arcy ve Devaraj, 2012; Hu vd., 2012; Willison ve Warkentin, 2013).

Bireylerin neden bilgi güvenliği ihlallerine karıştığını araştırmak için bir takım teoriler kullanılmıştır ancak bu teorilerden ikisi oldukça ön plandadır. Bunlar Genel Caydırıcılık Teorisi (GDT) (Erhlich, 1973) ve Koruma Motivasyon Teorisi (PMT)'dir (Rogers, 1975). Bu iki teori arasında bir takım benzerlikler ve farklılıklar bulunmaktadır. Örneğin her iki teori de özellikle kuruluş içinden güvenlik ihlallerinin nasıl önleneceğini araştırmak için kullanmaktadır. Buna karşılık PMT, bireyleri bilgi varlıklarını korumaya motive etmek için ne gerektiğini belirlerken GDT bireyleri bilgi güvenliği ihlalleri oluşturmaktan caydırmak için neler yapılabileceğine odaklanmaktadır (Johnston ve Warkentin, 2010; Straub, 1990).

2.5.1. Örgütsel Bilgi Güvenliği

Örgütler bir amacı olan, planlanarak oluşturulmuş ve dış paydaşlarla bağlantısı

bulunan yapılardır (Erdem, 2007). Örneğin işletmeler ve devlet kurumları örgüt olarak adlandırılabilir. Örgütlerin dış paydaşlarla iletişim halinde olması, iş yapması ve teknolojik cihazlara fazlasıyla ihtiyaç duyması örgüt içinde bilgi güvenliği noktasında hassasiyetleri artırmaktadır (Johnson ve Goetz, 2007). Bu nedenle örgütler güvenlik önlemlerini artırmak için bilgi güvenliği politikaları oluştururlar. Bilgi güvenliği politikası, "kuruluşlarının bilgi ve teknoloji kaynaklarını korumak için çalışanların rollerinin ve sorumluluklarının bir ifadesidir" (Bulgurcu vd., 2010). Chatterjee vd. (2015)'ye göre bir kuruluşun en zayıf halkası çalışanlarıdır. Bu nedenle, şirkette olan bir bilgi güvenliği politikası ihlali, bir çalışanın kuruluşun yerleşik bilgi güvenliği politikasına karşı olan herhangi bir eylemi olarak görülebilir (Hu vd., 2012). Araştırmalar bize, artık güvenli kanalların sadece güvenlik teknolojileri tarafından değil, aynı zamanda çalışanların yanlış davranışlarını kontrol ederek de yönlendirilmesi gerektiğini bildiriyor (Bulgurcu vd., 2010; D'Arcy vd., 2009; Siponen ve Vance 2010). Bunun yanısıra D'Arcy ve Lowry (2017)'ye göre bir bilgi güvenliği politikası, kurumsal teknoloji ve bilgi kaynaklarının uygun kullanımını belirtir. Bu nedenle kurumsal bir ortamda bilgi güvenliğine yönelik ana risk teknolojiden ziyade güvenlik olaylarına yol açan personelin eylemi veya eylemsizliğidir (Ghafir vd., 2016).

Özet olarak örgütsel bilgi güvenliği, örgüt içinde korunması gereken bilgilerin gerekli önlemler alınarak istenmeyen saldırılardan korunmasıdır. Bu da şirketlerde bilgi güvenliği yönetim sistemleriyle sağlanabilir. Bilgi güvenliği yönetim sistemlerinin oluşturulmasıyla tehditler tespit edilerek gerekli önlemler alınır ve bilgi güvenliği noktasında riskler en aza indirgenir (Vural ve Sağıroğlu, 2008). Bilgi güvenliği yönetimi etkin bir şekilde uygulamak için kurumsal yönetimin ilkeleri belirlenerek bu noktada çalışanlar bilinçlendirilmelidir. Belirtilen bu ilkeler kuruluşların bireysel bilgi yönetim mekanizmaları dâhil edilmelidir (Ali ve Green, 2007).

2.5.2. Bilgi Güvenliğini Tehdit Eden Unsurlar

Bilgi güvenliğini tehdit eden unsurlar kullanıcıların güvenlik hataları, güvenlik dikkatsizliği, güvenlik ihmali ve güvenlik saldırılarından oluşmaktadır (Leach, 2003). Teknolojinin hızlı değişimi ve gelişimi sebebiyle bilgi güvenliği tehditleri her geçen gün artmaktadır (Sudareswaran, 2018). Bu tehditler şirketlere geri dönüşü olmayan zararlar vermektedir. Bu durum şirketlerin iddiasına göre hem yasal ceza ve maliyet kayıplarına hem de şirketin geleceğini etkileyen durumlara sebebiyet vermektedir (Haslem vd., 2017). Örneğin Barrett vd. (2016)'e göre ihlaller sonucunda bir kurum itibarını kaybeder ve bu durum firmanın müşteri ile sorunlar yaşamaya başlamasına sebep olur.

Sonrasında ise müşteri şirkete olan güvenini kaybeder ve firmanın genel işleyişi bu durumdan olumsuz etkilenir. Buradan da anlaşılacağı gibi kurum içi bilgi suiistimali ve kurumsal bilgi teknolojilerinin varlıklarının kötüye kullanımı kuruluşlar arasında kritik bir sorun teşkil etmektedir (Baracaldo ve Joshi, 2013; Willison ve Warkentin, 2013).

Şirketlerin veri kaybı, bilgi güvenlik ihlalleri, sistem kesintileri, politika ihlalleri, ahlaki açıdan yozlaşmış eylemler ve bilgi güvenliği politikalarının kötüye kullanılması çoğunlukla şirket içindeki kişilerle ilişkilendirilmektedir. Kişilerin sebep olduğu ihlaller ciddi mali kayıplara ve itibar kaybına neden olmaktadır. Bu da kuruluşlar için büyük bir tehdit unsurudur (Wall ve Lyer, 2012).

2.5.3. Örgütler İçin Bilgi Güvenliği Farkındalığı ve Önemi

Bilgi güvenliği farkındalığı oluşturmanın en önemli amaçlarından biri örgütsel bilgi birikiminin doğru kullanılmamasından kaynaklı riskleri minimum seviyelere indirgemektir. Bunun yanında bilgi sistemleri kullanımında karşımıza çıkacak sıkıntılar hakkında bilgi sahibi olarak öncesinde çözümler bulmak ve örgütün bilgi güvenlik politikasına uyması adına katkı sağlamak diğer amaçlar arasında sayılabilir. Bilgi güvenliği farkındalık kavramı güvenliği riske atan durumlara karşı ne tür tedbirler alınabileceğini kapsayan bilgi güvenlik politikaları hakkında bilgi sahibi olunması şeklinde tanımlanabilir (Öztemiz ve Yılmaz, 2013).

Haeussinger ve Krang (2019)'a göre bilgi sistemleri güvenliği, dünya çapındaki şirketler için giderek daha kritik bir konu haline gelmektedir. Veri ihlalleri kurumların imajlarını yok eden, dolayısıyla ticari operasyonları kesintiye uğratan bir unsurdur. (Jeong vd., 2018). Agelidis (2016)'e göre, veri ihlallerinin verdikleri zararlar kalıcıdır ve ihlalleri geri almak imkânsızdır. Bu açıdan bakıldığında ihlaller şirketler açısından çok büyük kayıplara neden olmaktadır. Bu durum örgütler açısından bilgi güvenliğinin önemini göz önüne sermektedir. Li vd. (2019) çalışanların kurumlarına ait bilgi güvenliği politikası ve prosedürlerinden haberdar olduklarında siber güvenlik görevlerini yönetmek için kuruluşlarının siber güvenlik politikalarından haberdar olmayanlara göre daha bilgili oldukları görülmüştür. Bununla beraber kurumsal bilgi güvenliği ortamının çalışanların tehdit değerlendirmesi ve başa çıkma değerlendirmesi yeteneklerini olumlu yönde etkilediği kanaatine varılmıştır. Sonuç olarak, çalışanların bilgi güvenliği farkındalığının örgütlere olumlu katkısının olduğunu söyleyebiliriz. Araştırmalar çoğu kuruluşun işleyişinde bilgi güvenliği politikaları olsa bile, çalışanların düzenli olarak ve bilerek bu politikaları atlattığını ve göz ardı ettiğini göstermektedir (Bell vd., 2019; D'Arcy ve Lowry, 2017).

2.5.4. Bilgi Güvenliği İhlali Sonuçları

Bireyler için bilgilerini veya verilerini içeren bir kuruluşun bilgi teknolojileri güvenlik ihlalinden kaynaklanan zararları dört aşamada ifade edilebilir. Bunlar dolandırıcılık suçlamalarını çözmek için zaman ve para kaybı, gelecekteki kimlik hırsızlığına karşı bireylerin kendilerini korumaları için zaman ve para kaybı, hizmetleri kullanmanın veya ürünü satın almanın mali kaybı, kişisel bilgilerin kontrol kaybıdır (Romanosky, 2016). Bir başka araştırmada ihlallerin sebep olduğu kayıpların dokuz kaynaktan gelebileceğini öne sürülmektedir. Bunlar operasyonlardan kaynaklanan kayıplar, azalan gelirler, kötü karar verme nedeniyle oluşan fırsat kayıpları, bilgilerin ifşa edilmesinden kaynaklanan rekabet gücü kaybı, ihlal sırasında alınan maddi para veya mallardan kaynaklanan iş kayıpları, şirket itibarı kayıpları, mevcut hissedarların kayıpları, yasal kayıplar ve bilişim teknolojisi kayıplarıdır (Salmela, 2008).

Bilgi güvenlik ihlallerinin dünyadaki örneklerine bakacak olursak Çavuşoğlu vd. (2004)'ın çalışması göze çarpmaktadır. Buna göre piyasa değerinin güvenlik ihlallerinden nasıl etkilendiğini ölçen olay çalışmasında, internet güvenlik ihlallerini duyuran şirkete aşırı itibar kaybına mal olduğunu göstermiştir. Genel olarak, ihlali açıklayan şirketler, özellikle bunu duyurduktan sonraki ilk iki gün civarında, piyasa değerlerinde ortalama %2.1 kayıp yaşamıştırlar. Şirket her ihlal için yaklaşık 1,65 milyar dolar kaybetmiştir. Yapılan bir başka araştırma 12 aylık zaman diliminde 65 ülkede 2 216 veri ihlaliyle 53 308 güvenlik olayı olduğunu bildirmiştir. (Widep, 2018). Başka bir örnekte 2014 yılında Home Depot'un 56 milyon öğeye ait verileri ihlal edilmiştir ve bunun sonucunda 13 milyon dolarlık yasal ödemeyle sonuçlanmıştır. Başka bir ihlal olayında Nisan-Haziran 2011 arasında saldırıya uğrayan Sony'nin yaşadığı ihlal, açık ara en ünlü güvenlik saldırısıdır. Playstation ağı LulzSec tarafından kapatıldıktan sonra Sony'nin neredeyse 171 milyon dolar kaybettiği bildirilmiştir. Hack, 77 milyon hesabı etkilemiştir ve hala şimdiye kadarki en kötü oyun topluluğu veri ihlali olarak kabul edilmektedir (URL-1, 2016). Başka bir çalışmada, internetin alan adı sistemi (DNS) altyapısının çoğunu kontrol eden bir şirket olan Dyn, bir DDoS saldırısının kurbanı olmuştur. Dyn Company'nin sunucuları DDoS saldırısı altında kalmıştır ve bunun sonucunda The Guardian, Twitter, Netflix, GitHub, Spotify gibi şirket siteleri çökertilmiştir (URL-2, 2012). Günümüzde hala bu örnekler gibi birçok bilgi güvenliği ihlalleri ve doğurduğu geri dönüşü olmayan sonuçlar bulunmaktadır.

3. YÖNTEM

3.1. Araştırma Modeli

Araştırma modelinde tekno-stres bağımsız değişken, bilgi güvenliği politikası ihlali bağımlı değişken, tekno-gerilim ise aracı değişken olarak kullanılmıştır.

Şekil 1. Araştırma modeli

H1: Tekno-stres bilgi güvenlik politikası ihlaline neden olmaktadır.

H2: Tekno-stres teknojik gerilime neden olmaktadır.

H3: Tekno-stresin oluşturduğu teknolojik gerilim bilgi güvenliği ihlaline neden olmaktadır.

H4: Tekno-stres ile bilgi güvenlik politikası ihlalinde teknolojik gerilimin aracı rolü vardır.

3.2. Örneklem

Bu çalışmanın araştırma evrenini bilişim alanı çalışanları oluşturmaktadır. Bu doğrultuda çalışmanın araştırma grubunu Ankara, İstanbul, Kocaeli, İzmir, Trabzon ve Gümüşhane illerinde bilişim sektöründe aktif olarak çalışan 301 katılımcı oluşturmuştur.

3.2.1. Veri Toplama Yöntemi

Yapılan araştırmada veriler Türkiye'nin farklı illerinde bilişim sektöründe aktif olarak çalışan ve teknolojiyi kullanan katılımcılar arasından kolayda örneklem yöntemiyle toplanmıştır. Bu veriler çevrimiçi anket platformu aracılığıyla elde edilmiştir. Kolayda örnekleme aracılığıyla araştırma evreninde yer alan veriler basit, kısa zamanda ve ekonomik olarak elde edilir (Malhotra, 2004: 321). Araştırma kapsamında hazırlanan anket bilişim sektörünün sorunsallarını bireysel olarak ele almıştır. Bunun yanında ilgili anket araştırma sonuçlarını çözümlemeye yönelik elde edilen veriler ışığında hazırlanmıştır. Toplanan 361 veri içerisinden 60 veri uygun

olmadığı için analiz dışı bırakılmıştır. Bunun sonucunda kalan 301 veri analize dâhil edilmiştir.

3.2.2. Araştırmada Kullanılan Ölçekler

Brislin (1980)'in geri çeviri prosedürü önerilen tercüme ve geri tercüme prosedürüne göre yapılmış olup, buna göre ölçek ilk önce İngilizce'den Türkçe'ye daha sonrasında ise Türkçe'den İngilizce'ye çevirileri uygulanmıştır. Brilis'in geri çeviri prosedürü çeşitli alanyazında defalarca kullanılmıştır (Liu ve Keller 2021; Wang vd., 2018). Çalışmada tekno-gerilim, tekno-stres, bilgi güvenlik politikası ihlalleri ve birçok demografik maddeler ölçülmeye çalışılmıştır.

Tekno-stresi değerlendirdiğimiz ölçek Taraftar vd. (2007) tarafından geliştirilmiştir. Bu ölçek toplam 23 sorudan oluşmaktadır. Ölçek TAY (5 Soru), TI (4 Soru), TK (5 Soru), TGK (5 Soru) ve TB (4 Soru) olmak üzere toplam beş boyuttan oluşmaktadır. Yapılan birçok araştırmada (Fuglseth ve Sørebø, 2014; Wang vd. 2008; Zhao vd., 2020) çalışanların maruz kaldıkları teknolojilerden ötürü ne kadar stres yaşadıkları ölçülmeye çalışılmıştır. Ankete katılan çalışanlar soruları 5 puanlık bir ölçek üzerinden uygun gördükleri seçeneği işaretleyerek doldurmuşlardır (1-Kesinlikle Katılıyorum 2-Katılıyorum 3-Karasızım 4-Katılmıyorum 5-Kesinlikle Katılmıyorum). " Teknoloji, daha hızlı çalışmamı sağlıyor" ve "iş arkadaşlarım arasında, rekabetçi pozisyonlarını kaybetme korkusuyla, teknolojik konularda daha az bilgi paylaşımı yapıldığını düşünüyorum" örnek anket sorularıdır. Çalışmada kullanılan ölçekte Cronbach Alpha değerleri TAY:0.89, TI:0.81, TK:0.84, TGK:0.84, TB:0.82 olarak bulunmuştur (Tarafdar vd., 2007).

Tekno gerilimin değerlendirildiği ölçek ise Moore (2000) tarafından geliştirilmiş 5 maddelik iş tükenmişliği anketinin Nasirpouri vd. (2020) tarafından kısaltılarak 4 madde haline çevrilmiş halidir. Anketteki değerlendirmeler 5'li Likert tipi derecelendirme kullanılarak yapılmıştır. "Teknolojiyle ilgili faaliyetlerimden yorgun hissediyorum" ve "bütün gün farklı teknolojilerle çalışmak benim için bir yüktür" örnek anket sorularıdır. Orjinal çalışmada kullanılan ölçekte Cronbach Alpha değeri 0.94 olarak bulunmuştur (Nasirpouri vd., 2020).

Yapılan araştırmanın bağımlı değişkeni olan bilgi güvenliği politikası ihlalini test etmek için varsayımsal senaryo yaklaşımı uygulanmıştır. Bu yaklaşımın metodolojik olarak iyi bir seçenek olduğu görülmüştür (Straub ve Karahanna, 1998). Nitekim yapılan araştırmada gerçek dünyada karşı karşıya gelinen bilgi güvenlik ihlalleri ölçülmek istenmektedir. Bu yöntem katılımcılara gerçekçi durumların yazılı

açıklamalarını sunan ve ardından ilgilenilen bağımlı değişkenleri ölçen bir dizi derecelendirme ölçeğinde yanıtlar talep eden kısa hikâyelerden oluşmaktadır (Trevino, 1992: 127-128). Senaryo yönteminin kullanılması, kullanıcıların ahlaki olmayan davranışlarda bulunma isteğinin ölçümlenmesi, kararlara etki eden faktörlerin ayrıntılarının elde edilmesi ve sahip olunan algılarla gelecekteki davranışların ölçümlenmesi gibi avantajlar sağlamaktadır (Siponen ve Vance, 2010). Shadbad ve Biros (2020) altı farklı senaryo kullanarak sağlanan bu avantajdan yararlanarak BGPI ölçümlemişlerdir. Bu senaryolar parola yazma, parola paylaşımı, oturumu kapatmama, veri sızıntısı, USB kopyalama ve bağlantıya tıklama şeklindeki başlıklardan oluşmaktadır (D'Arcy vd., 2014; Siponen ve Vance, 2010).

Demografik değişken olarak araştırmada cinsiyet, yaş, eğitim durumu, meslek grubu, tecrübe, bulunduğu sektör, uyum eğitimleri, çalışan sayısı, uzaktan çalışma durumu, bilgi güvenlik politikaları gibi değişkenler olarak araştırılmıştır.

4. BULGULAR

4.1. Demografik Bulgular

Bu araştırma bilişim alanında çalışanları kapsamaktadır. Araştırmada cinsiyet, eğitim durumu, yaş, deneyim, meslek grupları, sektör, şirketteki çalışan sayıları, uzaktan çalışma, bilgi güvenlik politikası ve uyum eğitimi gibi unsurlar demografik değişkenler olarak ele alınmıştır. Bu araştırmanın demografik bilgilerinin dağılımı aşağıda belirtilen tablolarda verilmiştir.

Tablo 1. Demografik bulgular 1

	Sıklık	Yüzde	Gerçek Yüzde	Kümülatif Yüzde
Cinsiyet				
Erkek	212	70.4	70.4	70.4
Kadın	89	29.6	29.6	100.0
Toplam	301	100.0	100.0	

Tablo 1'de yer alan demografik bulgular incelendiğinde cinsiyete göre dağılımda erkeklerin oranı %70.4, kadınların oranı ise %29.6'dır.

Tablo 2. Demografik bulgular 2

Eğitim Durumu	Sıklık	Yüzde	Gerçek Yüzde	Kümülatif Yüzde
Lise	6	2.0	2.0	2.0
Ön Lisans	14	4.7	4.7	6.6
Lisans	218	72.4	72.4	79.1
Lisansüstü	63	20.9	20.9	100.0
Toplam	301	100.0	100.0	

Tablo 2'de yer alan demografik bulgular incelendiğinde çalışanların eğitim durumlarında lise eğitimine sahip çalışanların oranı %2.0, ön lisans eğitimine sahip çalışanların oranı %4.7, lisans eğitimine sahip çalışanların oranı %72.4, yüksek lisans eğitimine sahip çalışanların oranı ise %20.9'dur.

Tablo 3. Demografik bulgular 3

Meslek Grupları	Sıklık	Yüzde	Gerçek Yüzde	Kümülatif Yüzde
Bilgisayar Mühendisi	202	67.1	67.1	67.1

Tablo 3. (Devamı)

Meslek Grupları	Sıklık	Yüzde	Gerçek Yüzde	Kümülatif Yüzde
Yazılım Mühendisi	15	5.0	5.0	72.1
İş Analisti	15	5.0	5.0	77.1
Programcı	12	4.0	4.0	81.1
Bilişim Yöneticisi	12	4.0	4.0	85.0
Bilgi İşlem	11	3.7	3.7	88.7
Elektrik Elektronik	26	8.6	8.6	97.3
Endüstri Mühendisi	6	2.0	2.0	99.3
Matematik Mühendisi	2	0.7	0.7	100
Toplam	301	100.0	100.0	

Tablo 3'te yer alan demografik bulgular incelendiğinde çalışanların meslek gruplarına göre dağılımları görülmektedir. Buna göre bilgisayar mühendisi oranı %67.1, yazılım mühendisi oranı %5.0, iş analisti oranı %5.0, programcı oranı %4.0, bilişim yöneticisi oranı %4.0, bilgi işlem oranı %3.7, elektrik elektronik mühendisi oranı %8.6, endüstri mühendisi oranı %2.0, matematik mühendisi oranı %0.7'dir.

Tablo 4. Demografik bulgular 4

Çalıştığınız Sektör	Sıklık	Yüzde	Gerçek Yüzde	Kümülatif Yüzde
Bilişim Teknolojileri	200	66.4	66.4	66.4
Eğitim	15	5.0	5.0	79.7
Elektrik ve Elektronik	4	1.3	1.3	81.1
Enerji	27	9.0	9.0	90.0
Finans	6	2.0	2.0	92.0
İş ve Yönetim	16	5.3	5.3	97.3
Medya, İletişim ve Yayıncılık	2	0.7	0.7	98.0
Metal	4	1.3	1.3	99.3
Sağlık ve Sosyal Hizmetler	2	0.7	0.7	100
Spor ve Rekreasyon	6	2.0	2.0	68.4
Ticaret (Satış ve Pazarlama)	10	3.3	3.3	71.8
Toplumsal ve Kişisel Hizmetler	4	1.3	1.3	73.1
Ulaştırma, Lojistik ve Haberleşme	5	1.7	1.7	74.8
Diğer Sektörler	15	5.0	5.0	79.7
Toplam	301	100.0	100.0	

Tablo 4'te yer alan demografik bulgular incelendiğinde çalışanların sektör bilgisine göre dağılımları görülmektedir. Buna göre bilişim teknolojileri oranı %66.4, eğitim oranı %5.0, elektrik ve elektronik oranı %1.3, enerji oranı %9.0, finans oranı %2.0, iş ve yönetim oranı %5.3, medya, iletişim ve yayıncılık oranı %0.7, metal oranı %1.3, sağlık ve sosyal hizmetler oranı %0.7'dir. Buna ek olarak spor ve rekreasyon oranı %2.0, ticaret (satış ve pazarlama) oranı %3.3, toplumsal ve kişisel hizmetler %1.3, ulaştırma, lojistik ve haberleşme oranı %1.7, diğer sektörler oranı %5.0'dır.

Tablo 5. Demografik bulgular 5

Şirketlerdeki Çalışan Sayısı	Sıklık	Yüzde	Gerçek Yüzde	Kümülatif Yüzde
0-50	93	30.9	30.9	30.9
51-100	33	11.0	11.0	41.9
101-500	40	13.3	13.3	55.1
501-1000	41	13.6	13.6	68.8
1000 ve üzeri	94	31.2	31.2	100.0
Toplam	301	100.0	100.0	

Tablo 5'te yer alan demografik bulgular incelediğinde şirketlerdeki çalışanların sayısına ait dağılımlar görülmektedir. Buna göre 0-50 arası çalışanların oranı %30.9, 51-100 arası sahip çalışanların oranı %11.0, 101-500 arası çalışanların oranı %13.3, 501-1000 arası çalışanların oranı ise %13.6, 1000 ve üzeri çalışanların oranı %31.2'dir.

Tablo 6. Demografik bulgular 6

Uzaktan Çalışma	Sıklık	Yüzde	Gerçek Yüzde	Kümülatif Yüzde
Evet	138	45.8	45.8	45.8
Hayır	163	54.2	54.2	100.0
Toplam	301	100.0	100.0	

Tablo 6'da yer alan demografik bulgular incelendiğinde uzaktan çalışanların oranı %45.8, uzaktan çalışmayanları oranı ise %54.2'dir.

Tablo 7. Demografik bulgular 7

Bilgi Güvenliği Plitikası	Sıklık	Yüzde	Gerçek Yüzde	Kümülatif Yüzde
Evet	50	16.6	16.6	16.6
Hayır	251	83.4	83.4	100.0
Toplam	301	100.0	100.0	

Tablo 7'de yer alan demografik bulgular incelendiğinde bilgi güvenliği politikasına sahip şirketlerin oranı %16.6, bilgi güvenliği politikasına sahip olmayanların oranı ise %83.4'tür.

Tablo 8. Demografik bulgular 8

Oryantasyon Eğitimi	Sıklık	Yüzde	Gerçek Yüzde	Kümülatif Yüzde
Evet	113	37.5	37.5	37.5
Hayır	188	62.5	62.5	100.0
Toplam	301	100.0	100.0	

Tablo 8'da yer alan demografik bulgular incelendiğinde oryantasyon eğitimi alan çalışanların oranı %45.8, ortantasyon eğitimi almayan çalışanların oranı ise %54.2'dir.

Bu doğrultuda Türkiye'de farklı şehirlerdeki 301 bilişim personelinden elde edilen verilerle çalışmaya devam edilmiştir. Araştırmaya katılan kişilerin ortalama deneyim yılı 7.48'dir (Sd= 5.64 ve min. 1; max. 35). Yaş ortalaması ise 31.73 yıl olarak hesaplanmıştır (Sd= 6.17 ve min. 20; max. 58).

4.2. Tanımlayıcı İstatistikler

Ölçek sorularının SPSS 24 programı aracılığı ile analiz edildiği bu çalışmada tanımlayıcı istatistiklere ait en düşük çarpıklık katsayısı -1.27, en yüksek çarpıklık katsayısı 1.70'tir. Basıklık katsayılarına bakıldığında en düşük basıklık katsayısı -1.43, en yüksek basıklık katsayısı ise 3.39'dur. Elde edilen bulgular referans değer aralığına göre değerlendirildiğinde anket sorularına verilen yanıtların normal dağılım gösterdiği söylenebilir.

Tablo 9. Tanımlayıcı istatistikler

	Ortalama	Standart Sapma	Çarpıklık		Basıklık	
			İstatistik	Standart Sapma	İstatistik	Standart Sapma
TAY1	3.143	1.0967	-0.149	0.140	-1.093	0.280
TAY2	2.811	1.0835	0.256	0.140	-1.016	0.280
TAY3	2.934	1.0403	0.080	0.140	-1.147	0.280
TAY4	3.452	1.0240	-0.525	0.140	-0.636	0.280
TAY5	3.010	1.1532	0.007	0.140	-1.202	0.280
TI1	2.937	1.1370	0.124	0.140	-1.106	0.280
TI2	3.475	1.1476	-0.578	0.140	-0.772	0.280
TI3	3.359	1.1478	-0.349	0.140	-1.052	0.280
TI4	3.326	1.1577	-0.271	0.140	-1.073	0.280
TK1	2.409	1.1500	0.636	0.140	-0.459	0.280

Tablo 9. (Devamı)

	Ortalama	Standart Sapma	Çarpıklık		Basıklık	
			İstatistik	Standart Sapma	İstatistik	Standart Sapma
TK2	2.621	1.0997	0.400	0.140	-0.873	0.280
TK3	3.053	1.1123	-0.120	0.140	-1.101	0.280
TK4	2.272	0.9826	0.832	0.140	0.373	0.280
TK5	2.150	0.9060	0.945	0.140	0.717	0.280
TG1	2.216	0.9746	0.947	0.140	0.471	0.280
TG2	3.654	1.0771	-1.130	0.140	0.590	0.280
TG3	2.193	1.0406	0.787	0.140	-0.072	0.280
TG4	1.658	0.8119	1.643	0.140	3.392	0.280
TG5	2.598	1.2005	0.396	0.140	-0.912	0.280
TB1	3.774	0.8919	-1.073	0.140	1.093	0.280
TB2	3.432	1.0952	-0.584	0.140	-0.616	0.280
TB3	2.910	1.0561	0.146	0.140	-1.053	0.280
TB4	3.455	1.0403	-0.586	0.140	-0.578	0.280
ST1	2.558	1.0928	0.498	0.140	-0.673	0.280
ST2	2.837	1.1733	0.083	0.140	-1.205	0.280
ST3	2.661	1.1067	0.374	0.140	-0.822	0.280
ST4	2.495	1.0539	0.607	0.140	-0.396	0.280
AD1	2.970	1.5019	-0.091	0.140	-1.433	0.280
AD2	2.967	1.5337	-0.039	0.140	-1.489	0.280
ADG3	3.339	1.3385	-0.252	0.140	-1.062	0.280
JN1	1.558	1.0396	1.699	0.140	1.654	0.280
JN2	1.658	1.1630	1.706	0.140	1.763	0.280
JNG3	4.143	1.1844	-1.273	0.140	0.522	0.280
BR1	2.186	1.3851	0.769	0.140	-0.779	0.280
BR2	2.199	1.4260	0.797	0.140	-0.821	0.280
BRG3	3.708	1.1976	-0.745	0.140	-0.307	0.280
YS1	2.455	1.4383	0.439	0.140	-1.214	0.280
YS2	2.478	1.4573	0.450	0.140	-1.243	0.280
YSG3	3.744	1.2373	-0.778	0.140	-0.326	0.280
OR1	1.824	1.1940	1.267	0.140	0.453	0.280
OR2	1.817	1.2013	1.332	0.140	0.645	0.280
ORG3	4.080	1.1137	-1.106	0.140	0.394	0.280
KB1	1.910	1.1924	1.089	0.140	0.108	0.280
KB2	1.973	1.2540	1.112	0.140	0.088	0.280
KBG3	4.050	1.1608	-1.024	0.140	0.098	0.280
N	301					

Bu araştırma TST, BGPI ve TG değişkenlerinin birbirlerine olan etkileri üzerine yapılmıştır. Çalışmanın birinci kısmında ortak metod varyansı hatası kontrol edilmiştir. Devamında doğrulayıcı faktör analizi (DFA) yapılarak yapı geçerliliği değerlendirilmiştir. Sonrasında hipotezleri test etmek için SPSS 24 Hayes Process Model kullanılarak yapısal denklem modeli ve yol katsayıları analiz edilmiştir.

Katılımcıların değişkenleri hakkında veri almanın tek yolu olduğu zamanlarda anketler aracılığıyla verileri elde ederken ortak varyans hatasını incelemek önemli görülmektedir (Podsakoff vd., 2003). Ortak metod varyansı (CMV) harman tek faktör testi ve tek faktör ölçüm modeli olarak iki şekilde hesaplanmıştır. Harman tek faktör testi gerçekleştirildiğinde toplam varyansın % 50'den aşağısı gizil bir yapı tarafından açıklanıyorsa elde edilen bu sonuca göre mevcut çalışmada ortak yöntem varyansında problem olmadığı anlaşılmaktadır (Arasanmi ve Krishna, 2019; Baumgartner vd., 2021; Chen ve Fang, 2019; Dash ve Vohra, 2019). Harman tek faktör test ile 27 maddeye temel bileşenler analizi uygulanmıştır.

Döndürmesiz analiz sonuçları özdeğerleri birden büyük olmak şartıyla birlikte toplam varyansın % 62.41'ini açıklamaktadır. İlk faktör varyansın % 27.52'sini oluşturmuştur. İkinci aşamada tek faktörlü (X2: 276.864; $\chi 2$ / df: 7.339; $p< 0.01$; CFI: 0.475; TLI: 0.434; GFI: 0.617, RMSEA: 0.135) ve yedi faktörlü model (X2: 657.844; $\chi 2$ / df: 2.175; $p< 0.01$; CFI: 0.919; GFI:0.877; TLI:0.905; RMSEA: 0.058) verileri kıyaslandığında uyum iyilik değerinin son derece zayıf olduğu görülmüştür. Bu nedenle yapılan araştırmada ortak yöntem varyansının problem olmadığı ortaya çıkmıştır. Çalışmanın devamında çarpıklık ve basıklık değerleri incelenerek veri setinin dağılımının normal olup olmadığı test edilmiştir. Veriler analize hazır hale getirildikten sonra veri setinin çarpıklık ve basıklık değerlerine bakılarak dağılım test edilmiştir. Yapılan çalışmalarda çarpıklık ve basıklık değerleri ile ilgili basıklık değerinin 5'ten küçük olması halinde veri setinin normal dağıldığı (Byrne, 2010), çarpıklık değerinin ±3 ve basıklık değerinin ise ± 10 aralığında olmasının veri setinin normal dağıldığını görmek için yeterli olduğu ifade edilmektedir (Kline, 2016). Bu bilgiler dikkate alındığında çarpıklık ve basıklık değerleri sırasıyla TAY = -0.222 , -0.436; TK = 0.545, 0.523; TB = -0.553, -0.139; TI = -0.241, -0.646; TGK = 1.157, 1.605; TG = 0.295, -0.474 ve BGPI = 0.615, -0.351 değerleridir. Bulunan çarpıklık ve basıklık değerleri araştırmada kullanılan veri setinin normal dağıldığını göstermektedir.

Tablo 10. Doğrulayıcı faktör analizi

Ölçüm Modeli	DF	CMIN	CMIN/DF	P < 0.05	CFI	GFI	TLI	RMSEA
Tek Faktör Modeli	377	276.864	7.339	0	0.475	0.617	0.434	0.135
İki Faktör Modeli	376	2547.342	6.775	0	0.523	0.646	0.485	0.129
Üç Faktör Modeli	374	2277.129	6.089	0	0.582	0.682	0.546	0.121
Dört Faktör Modeli	371	2125.186	5.728	0	0.615	0.707	0.578	0.117
Beş Faktör Modeli	367	1876.997	5.114	0	0.668	0.749	0.633	0.109
Altı Faktör Modeli	362	1459.160	4.031	0	0.759	0.810	0.730	0.093
Yedi Faktör Modeli	302	657.844	2.175	0	0.919	0.877	0.905	0.058

Not: n = 301. CFI = Karşılaştırmalı uyum indeksi; GFI = Uyum iyiliği indeksi; TLI: Normlandırılmamış uyum indeksi; RMSEA = Yaklaşık hataların ortalama karekökü.

4.3. Doğrulayıcı Faktör Analizi

Araştırmada yapılan ölçümlere Doğrulayıcı Faktör Analizi (DFA) uygulanarak yapı geçerliliği değerlendirilmiştir. Elde edilen sonuçlar incelendiğinde, yedi faktörlü modelin uyum iyiliği göstergelerinin belirlenen iyi model uyum iyiliği değerlerine sahip olduğu bulunmuştur (X^2 : 508.715; $\chi 2$ / df: 2.00; $p< 0.01$; CFI : 0.92; TLI : 0.92; SRMR : 0.06; RMSEA : 0.06). Ayrıca değişkenlerin (TAY, TI, TK, TGK TB, TG ve BGPI) birbirleriyle aynı değişkenler olmadığı görülmüştür. Yapılan incelemelerde faktör yükünün 0.50'den küçük olmasından kaynaklı iki soru yapılan analizden çıkarılmıştır. Bu iki madde TAY4 ve TGK2 olarak isimlendirilmiştir. Bunun dışında bütün değişkenler yapılan analizde kullanılmıştır. Gizli değişkenlerin göstergelerinin faktör yüklerinin anlamlı olduğu bulunmuştur. Faktör yükleri, TAY 0.64-0.78, TI 0.63-0.80, TK 0.54-0.77, TGK 0.57-0.88, TB 0.62-0.84, TG 0.62-0.84 ve BGPI 0.98-0.93 aralıklarında bulunmuştur. Elde edilen değer aralıklarının iç tutarlılığı sağladığı görülmüştür. Doğrulayıcı faktör analizi kapsamında analiz edilen ölçüm modeline ait boyutların açıklanan ortalama varyans (AVE) değerinin 0.50 ve üzerinde (Hair vd, 1995:642) olması ve birleşik güvenilirlik katsayılarının (CR) değerinin 0.60 üzerinde olması gerekmektedir (Bagozzi ve Yi, 1988). Araştırmadaki değişkenlerin AVE ve CR değerlerinin $0.43<AVE<0.91$ ve $0.76<CR<0.96$ aralıklarında olduğu bulunmuştur. CR değerinin AVE değerinden büyük olması şartını sağlayan ölçüm modelinin bütünleşik güvenilirliği incelenmiş ve CR değerlerinin 0.60 üzerinde olması nedeniyle içsel tutarlılık doğrulanmıştır (Hair vd., 2019). Ayrışma geçerliliğinde ise Fornell ve Larcker (1981) kriterinden yararlanılmıştır. Fornell ve Larcker (1981) kriteri dikkate alındığında çalışmada yer alan yapıların AVE değerlerinin karekökünün korelasyondan daha yüksek olduğu görülmüştür. Sonuç olarak araştırmada yer alan tüm değişkenlerin ayrışma geçerliliğini sağladığını görülmüştür.

Tablo 11. Doğrulayıcı faktör analizi sonuçları

Değişkenler	Ort	Faktör Yükü	Cronbach σ	CR	AVE
Tekno-İş yükü			0.78	0.76	0.47
TAY3	2.93	0.79			
TAY2	2.81	0.78			
TAY1	3.14	0.61			
TAY5	3.01	0.53			
Tekno-İstila			0.81	0.81	0.51
TI4	3.32	0.78			
TI3	3.35	0.73			
TI1	2.93	0.69			
TI2	3.47	0.65			
Tekno-Karmaşıklık			0.79	0.79	0.44
TK5	2.15	0.78			
TK2	2.62	0.69			
TK3	3.05	0.63			
TK4	2.27	0.62			
TK1	2.21	0.53			
Tekno-Güvensizlik			0.74	0.77	0.47
TG1	2.21	0.79			
TG3	2.19	0.73			
TG4	1.65	0.59			
TG5	2.59	0.50			
Tekno-Belirsizlik			0.78	0.77	0.47
TB2	3.43	0.91			
TB1	3.77	0.68			
TB4	3.45	0.58			
TB3	2.91	0.51			
Tekno-Gerilim			0.90	0.90	0.68
TG4	2.49	0.87			
TG1	2.55	0.86			
TG2	2.83	0.82			
TG3	2.66	0.71			
Bilgi Güvenlik Politikası İhlali			0.95	0.96	0.92
SEN2	2.18	1.01			
SEN1	2.15	0.90			

Not: TAY: Tekno-İş yükü, TI: Tekno-İstila, TK: Tekno-Karmaşılık; TGK: Tekno-Güvensizlik, TB: Tekno-Belirsizlik, TG: Tekno-Gerilim ve SEN: Senaryo. X2: 508.715; $\chi 2$ / df: 2.00; $p< 0.01$; CFI: 0.92; TLI: 0.92; SRMR: 0.06; RMSEA: 0.06* Tüm faktör yükleri 0,001 düzeyinde anlamlıdır.

Tablo 11 incelendiğinde araştırma modelinin uygun içsel tutarlılığa ve güvenilirliğe, ayrışma geçerliliğine ve yakınsak geçerliliğe sahip olduğu görülmüştür.

4.4. Yapının Özellikleri ve Korelasyon

Bu araştırmada yer alan bütün değişkenlerin ifade edilen ayırt edici geçerlilik seviyesini sağladığı görülmektedir. Sonuç olarak ifade edilen çalışma modelinin taşıması gereken ayırt edici geçerliliğe, güvenilirliğe, yakınsak geçerliliğe ve iç tutarlılığa sahip olduğu sonucuna ulaşılmıştır. Bundan dolayı ortaya çıkan bu veriler araştırma hipotezini ölçmek için oldukça tutarlı bir sonuç sunmaktadır.

Tablo 12. Yapının özellikleri ve korelasyonları

Değişkenler	Ort	SD	AVE	1	2	3	4	5	6	7
TAY	2.97	0.85	0.78	1						
TI	3.27	0.91	0.72	0.44**	1					
TK	2.50	0.78	0.66	0.27**	0.37**	1				
TG	2.02	0.77	0.69	0.18**	0.27**	0.60**	1			
TB	3.39	0.79	0.69	0.04	0.12*	-0.03	0.27			
TG	2.63	0.96	0.83	0.38**	0.48**	0.50**	0.44**	-0.03	1	
BGPI	2.16	0.83	0.96	0.10	0.17**	0.25**	0.39**	-0.09	28**	1

Not: TAY:Tekno-İş yükü, TI:Tekno-İstila, TK:Tekno-Karmaşıklık; TGK:Tekno-Güvensizlik, TB:Tekno-Belirsizlik, TG:Tekno-Gerilim ve BGPI:Bilgi Güvenlik Politikası İhlali.

Tablo 12'de belirtildiği gibi, TAY; TI($r = 0.44$, $p<0.01$), TK($r = 0.27$, $p<0.01$), TGK($r = 0.18$, $p<0.01$) ve TG($r = 0.38$, $p<0.01$) ile pozitif yönlü ilişki vardır. TI; TK($r = 0.37$, $p<0.01$), TGK($r = 0.27$, $p<0.01$), TB($r = 0.12$, $p<0.05$), TG($r = 0.48$, $p<0.01$) ve BGPI($r = 0.17$, $p<0.01$) ile pozitif yönlü ilişki vardır. TK; TGK($r = 0.60$, $p<0.01$), TG($r =0.50$, $p<0.01$) ve BGPI($r = 0.25$, $p<0.01$) ile pozitif yönlü ilişki vardır. TGK; TG($r = 0.44$, $p<0.01$) ve BGPI($r = 0.39$, $p<0.01$) ile pozitif yönlü ilişki vardır. TG ile BGPI($r = 0.28$, $p<0.01$) ile pozitif yönlü ilişki vardır. Sonuçlar hipotezimizi test etmek için istenileni bize sunmaktadır.

4.5. Hipotez Testi

Aracılık etkisi konusunda çalışma yapan Baron ve Kenny (1986) aracılığın geçerli kabul edilebilmesi için dört koşul ortaya koymuştur. Bunlar bağımlı ve bağımsız değişkenlerin anlamlı bir ilişkisinin olması, aracı değişken ve bağımsız değişken arasındaki ilişkinin anlamlı olması, bağımlı değişken ve aracı değişken arasındaki ilişkinin anlamlı olması ve modellemeye aracılık etkisini yapacak olan değişkenin eklenmesi durumunda bağımlı ve bağımsız değişken arasındaki ilişki gücünün yok olma durumudur. Bu durumda tam aracılık etkisinden söz edilirken ilişki gücünün önemli oranda azaldığı zamanda ise kısmı aracılık etkisinden söz edilmektedir.

İlk olarak, TST ile BGPI arasında pozitif ilişki olacağı beklenmektedir. Yapılan regresyon analizinde TST ile BGPI arasındaki ilişkinin anlamlı olduğu görülmüştür ($R2 = 0.12$, $F(20.42) = 5.73$, $p<0.001$). Sonuçlar ($\beta = 0.31$, $p<0.001$), yüksek TST düzeyi ile BGPI arasında pozitif ilişki olduğunu göstermiştir. Buradan çıkarımla H1 hipotezi desteklenmiştir. İkinci olarak, TST ile TG arasında pozitif ilişki olacağı beklenmektedir. Yapılan regresyon analizinde TST ile TG arasındaki ilişkinin anlamlı olduğu görülmüştür ($R2 = 0.37$, $F(84.61) = 12.82$, $p<0.001$). Sonuçlar ($\beta = 0.60$, $p<0.001$), yüksek TST düzeyi ile TG arasında pozitif ilişki olduğunu göstermiştir. Buradan

çıkarımla H2 hiptezi de desteklenmiştir. Üçüncü olarak, TG ile BGPI arasında pozitif ilişki olacağı beklenmektedir. Yapılan regresyon analizinde TG ile BGPI arasındaki ilişkinin anlamlı olduğu görülmüştür ($R2= 0.13$, $F(20.81) = 5.79$, $p<0.001$). Sonuçlar($\beta = 0.32$, $p<0.001$), yüksek TG düzeyi ile BGPI arasında pozitif ilişki olduğunu göstermiştir. Buradan çıkarımla H3 hipotezi desteklenmiştir. Tablo 12'de aracılık analizinde kullanılan sonuçlar açıklanmıştır. Son olarak, TG değişkeninin TST ile BGPI arasında aracılık edeceği düşünülmüştür. Aracılık etkisinden bahsedebilmek için TST'nin TG'yi büyük oranda etkilemesi gerekmektedir. Bunun yanında, TG yokluğunda TST BGPI'ya önemli ölçüde etki etmektedir. BGPI üzerinde TST ve TG birlikte modele eklenirse teknostresin etkisini öncekine oranla kaybettiği gözlemlenmiştir. Bununla birlikte %95 güven aralığında 5000 altörneklemli önyükleme işlemi yapılarak dolaylı etkilerin aralık hesaplanması yapılmıştır (Cepeda-Carrion vd., 2017). Önyükleme yapmak dolaylı etkilerden bazıları için CI'leri hesaplamak adına iyi bir yoldur (Williams ve MacKinnon, 2008). Elde edilen sonuçlara göre, önyükleme testinde TG'nin dolaylı etkisinin 0.06 ile 0.34 aralığında olduğu tespit edilmiştir. Önyükleme analizi sonucunda sıfır elde edilmediği için TST ve BGPI arasında kısmi bir aracılık etkisi olduğu kanısına varılmıştır. Önyükleme analizinin istatiksel sonuçlarına göre sonuçların TG üzerinde anlamlı dolaylı etkilerinin olduğu ve H4 hipotezinin desteklendiği bulunmuştur.

Tablo 13. Aracılık analizi sonuçları

Öncüller			Tekno-gerilim				Bilgi Güvenlik Politikaları İhlali					
	β	**SE**	**t**	**LLCI**	**ULCI**	**R^2**	**β**	**SE**	**t**	**LLCI**	**ULCI**	**R^2**
TST	0.58***	0.09	12.21	0.91	1.26	0.33	0.15*	0.11	2.24	0.03	0.46	0.10
TG							0.17**	0.06	2.92	0.06	0.28	
F	149.145***						15.78***					
TST-BGPI	0.26***	0.09	4.74	0.25	0.61	0.07						
F	22.480**											
TG-BGPI	0.29***	0.05	5.11	0.15	0.34	0.08						
F	26.20***											
Tahmin				**Etki**		**SE**		**LLCI**			**ULCI**	
Doğrudan etki												
TST→BGPI				0.25		0.11		0.03			0.46	
Dolaylı etki												
TST-TG-BGPI				0.18		0.07		0.05			0.32	
Toplam etki												
TST→BGPI				0.43		0.09		0.25			0.61	

Not:TST:Tekno-stres,TG:Tekno-gerilim ve BGPI:Bilgi Güvenlik Politikası İhlali

5. TARTIŞMA

Tekno-stresin bilgi güvenlik ihlali etkisinde tekno-gerilimin aracı rolünün incelendiği bu araştırmada tekno-stres ile bilgi güvenlik politikası ihlalinde tekno-gerilim değişkeninin kısmi aracı rolü tespit edilmiştir. Bunun yanında tekno-stres değişkeni ile tekno-gerilim arasında pozitif yönlü anlamlı ilişkiler olduğu görülmüştür. Yine araştırma sonuçlarına göre tekno-stres ile bilgi güvenlik politikaları ihlali arasında pozitif yönlü anlamlı bir ilişkiler olduğu belirlenmiştir. Son olarak araştırma değişkenlerinden tekno-gerilim ile bilgi güvenlik politikaları ihlali arasında pozitif yönlü bir ilişki olduğu tespit edilmiştir. Araştırmaya dair elde edilen bulgular alanyazındaki diğer araştırma sonuçları doğrultusunda aşağıdaki gibi tartışılmıştır.

Araştırmanın ilk sonucuna göre tekno-stres ile tekno-gerilim arasında pozitif yönlü anlamlı bir ilişki mevcuttur. Bu sonuç alanyazındaki benzer araştırma sonuçlarıyla desteklenmektedir (Boyer-Davis, 2018; Galluch vd., 2015; Hauk vd., 2019; Lee vd., 2016; Srivastava vd., 2015). Ayyagari vd. (2011) yaptıkları çalışmada bilişim çalışanlarının teknoloji kullanımı nedeniyle önemli ölçüde gerginlik yaşadıklarını ve bu durumun çalışanlar üzerinde strese sebebiyet verdiğini tespit etmişlerdir. Teknolojinin sürekli olarak yenilenmesi ve gelişmesi örgüt çalışanlarının bu sürece ayak uydurmasını zorlaştırabilmektedir. Bu zorluk çalışanlarda tekno-gerilim ile sonuçlanabilir.

Araştırmadan elde edilen bir diğer sonuç tekno-stres ile bilgi güvenlik politikaları ihlali arasında pozitif yönlü anlamlı ilişkiler olduğunu ortaya koymaktadır. Bu araştırma bulgusu alanyazındaki benzer araştırma sonuçlarıyla uyum göstermektedir (D'Arcy vd., 2014; Park ve Cho, 2016; Shadbad ve Biros, 2020). Siponen ve Vance'nin 2010'da yaptıkları çalışmada bilgi güvenliği noktasında oluşan ihlallerin çalışanların tekno-stres düzeylerini artırdığını tespit etmişlerdir. Bu durum çalışanların yaşadığı teknoloji yorgunluğunun bir dışavurumu olarak açıklanabilir.

Yapılan çalışmada tekno-gerilim ile bilgi güvenlik politikaları ihlali arasında pozitif yönlü anlamlı bir ilişkiler olduğu görülmüştür. Bu sonuç alanyazındaki benzer araştırma sonuçları tarafından desteklenmektedir (ör: Nisafani vd., 2020). Chesley'in (2014) yaptığı araştırmada yüksek düzeydeki tekno-gerilimin bilgi güvenlik ihlaline yol açtığı tespit edilmiştir. Bu bulgu çalışanlarda gerginliğin sebep olduğu fiziksel ve bedensel etkileşimin bilgi güvenliği ihlaline sebep olmasıyla ile açıklanabilir.

Yapılan araştırmadan elde edilen sonuçlara göre tekno-stres ile bilgi güvenlik politikası ihlalinde tekno-gerilim değişkeninin kısmi aracı rolü olduğu belirlenmiştir. Bu

bulgu bilişim sektöründe çalışanların teknolojiye aşırı düzeyde maruz kalmalarından kaynaklanabilir. Bu maruz kalma çalışanlar üzerinde ciddi düzeyde iş gerilimine sebep olarak onların hata yapma olasılıklarını artırabilir. Bu durum da bilgi güvenliği noktasında zafiyet oluşturabilir. Bu bulguya paralel araştırma sonuçlarının alanyazında oldukça sınırlı olduğu görülmüştür (Islam vd., 2018). Örneğin Gaudioso vd. (2017)'nun yaptıkları çalışmada tekno-stresin ve tekno-gerilimin örgütlerde istenmeyen olumsuz sonuçlara sebep olabileceği bulgulanmıştır. Bu araştırma sonuçlarının aksine Shadbad ve Biros'un (2020) yaptıkları çalışmada gerginliğin tekno-stres ile bilgi güvenliği ihlali arasındaki ilişkiye aracılık etmediği görülmüştür.

6. SONUÇ VE ÖNERİLER

Araştırmanın bu bölümünde yapılan çalışmadan elde edilen sonuçlar kısaca belirtilmiştir. Bunun yanında araştırmadan elde edilen sonuçlara dayalı olarak geliştirilen öneriler sıralanmıştır. Yapılan araştırma sonucunda;

1. Tekno-stres ile bilgi güvenliği ihlali arasındaki ilişkide tekno-gerilim değişkeninin kısmi aracı bir rolü olduğu belirlenmiştir.

2. Tekno-stres seviyesi ile tekno-gerilim düzeyi arasında pozitif yönlü anlamlı ilişkiler olduğu tespit edilmiştir.

3. Tekno-stres seviyesi ile bilgi güvenliği ihlali değişkeni arasında pozitif yönlü anlamlı ilişkiler olduğu belirlenmiştir.

4. Tekno-gerilim düzeyi ile bilgi güvenliği ihlali değişkeni arasında pozitif yönlü anlamlı ilişkiler olduğu tespit edilmiştir.

Araştırmadan elde edilen sonuçlara dayalı olarak uygulama sahasında olan örgüt yönetimlerine ve araştırmacılara bazı öneriler sunulmaktadır. Bu çerçevede;

1. Çalışanların yüksek düzeyde tekno-stres yaşamalarına sebep olabilen bilgi eksikliği ve farkındalıkların artırılabilmesi adına çalışanlar düzenli aralıklarla hizmet içi eğitimlere alınabilir.

2. Örgütlerde kullanılan bilişim sistemlerinde güncel işletim sistemleri ve anti-virüs programlarının kullanılması sağlanabilir.

3. Stresin iş yeri ortamında daha iyi yönetilebilmesi için çalışanlara psiko-eğitimsel destek sağlanması noktasında gerekli girişimlerde bulunulabilir.

4. Bu araştırmada tekno-stres ile ilişkili olan bilgi-güvenlik ihlali ve tekno-gerilim değişkenleri çalışılmıştır. İleride yapılacak araştırmalarda tekno-strese etki eden farklı değişkenler araştırılabilir.

5. Bu araştırma bilişim sektörünün kullanıldığı farklı departmanlarda yapılarak ortaya nasıl bir etkinin çıkacağı araştırılabilir.

6. İleride yapılacak araştırmalarda nitel araştırma yöntemlerinden yararlanılarak tekno-stresin çalışanlar üzerinde nasıl etkiler oluşturabildiği derinlemesine bir şekilde çalışılabilir.

KAYNAKÇA

Agelidis, Y. (2016). Protecting the good, the bad, and the ugly exposure data breaches and suggestions for coping with them. *Berkely Technology Law Journal 2016 Special Issue.* 31(2), 1057-1078.

Ahmed, M., Sharif, L., Kabir, M. ve Al-Maimani, M. (2012). Human errors in ınformation security. *International Journal of Advanced Trends in Computer Science and Engineering*, 1(3), 82-87.

Akay, İ. G. (2014). Bilgi güvenliği yönetim sistemleri: Bilgi güvenliği uygulama mülakatları. Yüksek lisans tezi, Yükseköğretim Kurulu Ulusal Tez Merkezi, (368390).

Ali, S. ve Green, P. (2007). IT governance in public sector organizations. An Australian context. *Journal of Global Information Management*, 15(4), 41-63.

Arasanmi, C. N. ve Krishna, A. (2019). Employer branding: Perceived organisational support and employee retention the mediating role of organisational commitment. *Industrial and Commercial Training*, 51(3), 174-83.

Arnetz, B. B. ve Wiholm, C. (1997). Technological stress: Psychophysiological symptoms in modern offices. *Journal of Psychosomatic Research,* 43(1), 35-42.

Atanasoff, L. ve Venable, M. A. (2017). Technostress: Implications for adults in the workforce. *The Career Development Quarterly*, 65(4), 326-338.

Ayyagari, R., Grover, V. ve Purvis, R. (2011). Technostress: Technological antecedents and implications. *MIS Quarterly*, 35(4), 831-858.

Bagozzi, R. P. ve Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74-94.

Baracaldo, N. ve Joshi, J. (2013). An adaptive risk management and access control framework to mitigate insider threats. *Computers and Security*, 9, 273-254.

Baron, R. M., ve Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic and statistical considerations. *Journal of Personality and Social Psychology*, 51, 1173-1182.

Barrett, M., Garrety, K. ve Seberry, J. (2016). ICT professionals' perceptions of responsibility for breaches of computer security. 20 Eylül 2022 tarihinde https;//www.researcgate.net/publication/ 30385937 adresinden erişildi.

Baumgartner, H., Weijters, B. ve Pieters, R. (2021). The biasing effect of common method variance: Some clarifications. *Journal of the Academy of Marketing Science*, 49(2), 221-35.

Bell, A. J. C., Rogers, M. B. ve Pearce, J. M. (2019). The insider threat: Behavioral indicators and factors influencing likelihood of intervention. *International Journal of CriticalInfrastructure Protection,* 24, 166–176.

Boyer-Davis, S. (2018). The relationship between technology stress and leadership style: An empirical investigation. *Journal of Business and Educational Leadership,* 8(1), 48-49.

Brand, S. (2000, June 19). *The long now foundation.* 20 Aralık 2022 tarihinde www.longnow.org: longnow.org/essays/technology-moving-too-fast/ adresinden erişildi.

Brislin, R. W. (1980). Expanding the role of the interpreter to include multiple facets of intercultural communication. *International Journal of Intercultural Relations*, 4(2), 137-48.

Brod, C. (1984). *Technostres: The Human Cost of Computer Revolution.* Michigan: Addison-Wesley.

Brown, R., Duck, J. ve Jimmieson, N. (2014). E-mail in the workplace: The role of stress appraisals and normative response pressure in the relationship between email stressors and employee strain. *International Journal of Stress Management*, 21(4), 325-347.

Bulgurcu, B., Cavusoglu, H. ve Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.

Byrne, B. M. (2010). *Structural Equation Modeling with Amos*. New york: Routledge Taylor & Francis Group.

Califf, C. B., Sarker, S. ve Sarker, S. (2020). The bright and dark sides of technostress: A mixed-methods study involving healthcare. *MIS Quarterly*, 44(2), 809-856.

Cavusoglu, H., Cavusoglu, H. ve Raghunathan, S. (2004). Economics of it security management: Four improvements to current security practices. *Communications of the Association for Information Systems*, 14, 65-75.

Carrion, G. C., Nitzl, C. ve Roldan, J.L. (2017). Mediation Analyses in Partial Least Squares Structural Equation Modeling: Guidelines and Empirical Examples. *Partial Least Squares Path Modeling*: *Basic concepts, methodolojical issues and applications,* 173-195.

Champion, S. (1988). Technostress: Technology's toll. *School Library Journal*, 35(3), 48-51.

Chandra, S., Shirish, A. ve Srivastava, S. C. (2019). Does technostress inhibit employee innovation? Examining the linear and curvilinear influence of technostress creators. *Communications of the Association for Information Systems*, 44(1), 299-331.

Chatterjee, S., Sarker, S. ve Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, 31(4), 49-87.

Chen, H. L. ve Fang, S. C. (2019). Interaction effect of leader-member exchange and stress mindset on challenge stressor and job performance relationship. *Research Journal of Business and Management*, 6(4), 281-90.

Chen, X., Chen, L. ve Wu, D. (2018). Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective. *Journal of Computer Information Systems*, 58(4), 312-24.

Chesley, N. (2014). Information and communication technology use, work intensification and employee strain and distress. *Work, Employment and Society*, 28(4), 589-610.

Clark, K. ve Kalin, S. (1996). Technostressed out? How to cope in the digital age. *Library Journal*, 121(13), 30-32.

Cooper, C. L., Dewe, P. J. ve O'Driscoll, M. P. (2002). *Organizational Stress: A Review and Critique of Theory, Research and Applications*. California: Sage.

Çalışkan, M. (2022). Öğretmen adaylarının teknostres düzeylerinin belirlenmesi. Doktora tezi, Yükseköğretim Kurulu Ulusal Tez Merkezi, (715328).

Çek, E. (2017). Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği için insan faktörünün önemi ile ilgili çalışma. Yüksek lisans tezi, Yükseköğretim Kurulu Ulusal Tez Merkezi, (496021).

Çetin, D. ve Bülbül, T. (2017). Okul yöneticilerinin teknostres algıları ile bireysel yenilikçilik özellikleri arasındaki ilişkinin incelenmesi. *Abant İzzet Baysal Üniversitesi Eğitim Fakültesi Dergisi*, 17(3), 1241-1264. https://doi.org/10.17240/aibuefd.2017.17.31178-338821

Çoklar, A. N., Efilti, E., Şahin, Y. L. ve Akçay, A. (2016). Determining the reasons of technostress experienced by teachers: A qualitative study. *Turkish Online Journal of Qualitative Inquiry*, 7(2), 71-96.

D'Arcy, J., Hovav, A. ve Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98.

D'Arcy, J. ve Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. Decision Sciences, 43(6), 1091-1124.

D'Arcy, J. ve Lowry, P. B. (2017). Cognitive affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Information Systems Journal, 29(1), 1-27.

D'Arcy, J., Tejaswini, H. ve Mindy, K. S. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, 31(2), 285-318.

Dash, S. S. ve Vohra, N. (2019). The leadership of the school principal: Impact on teachers' job crafting, alienation and commitment. *Management Research Review*, 42(3), 352-369.

Doğrular, M. M. (2019). Teknostresin verimlilik üzerine etkisi. Doktora tezi, Yükseköğretim Kurulu Ulusal Tez Merkezi, (574148).

Ehrlich, I. (1973). Participation in illegitimate activities: A theoretical and empirical investigation. *Journal of Political Economy*, 81(3), 521-565.

Eppler, M. J. ve Mengis, J. (2004). The concept of information overload: A review of literature from organization science, accounting, marketing, MIS, and related disciplines. *The Information Society*, 20(5), 325-344.

Erdem, R. (2007). Örgüt kültürü tipleri ile örgütsel bağlılık arasındaki ilişki: Elazığ il merkezindeki hastaneler üzerinde bir araştırma, *Eskişehir Osman Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 2(2), 63–79.

Erdoğan, T., Ünsar, S. ve Süt, N. (2009). Stresin çalışanlar üzerindeki etkileri: Bir araştırma. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 14(2), 447-461.

Fieseler, C., Grubenmann, S., Meckel, M. ve Muller, S. (2014). The leadership dimension of coping with technostress. 47th Hawaii International Conference on System Sciences, 6-9 January 2014, Hawaii, s. 530-539.

Forman, C., King, J. L. ve Lyytinen, K. (2014). Special section introduction: Information, technology and the changing nature of work. *Information Systems Research*, 25(4), 789-95.

Fornell, C. ve Larcker D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39-50.

Fuglseth, A. M. ve Sørebø, Ø. (2014). The effects of technostress within the context of employee use of ICT. *Computers in Human Behavior*, 40, 161-70.

Fussell, R. S. (2005). Protecting information security availability via self-adapting intelligent agents. Military Communications Conference, 17-20 October 2005, Atlantic City, s. 1-6.

Galluch, P. S., Grover, V. ve Thatcher, J. B. (2015). Interrupting the workplace: Examining stressors in an information technology context. *Journal of the Association for Information Systems*, 16(1), 1-47.

Gaudioso, F., Turel, O. ve Galimberti, C. (2017), The mediating roles of strain facets and coping strategies in translating techno-stressors into adverse job outcomes, *Computers in Human Behavior*, 69, 189-196.

Ghafir, I., Prenosil, V., Alhejailan, A. ve Hammoudeh, M. (2016). Social engineering attack strategies and defence approaches. 4th International Conference on Future Internet of Things and Cloud, 22-24 August 2016, Canada, s. 145-149.

Gülmüş M. (2010). Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği. Yüksek lisans tezi, Yükseköğretim Kurulu Ulusal Tez Merkezi, (295662).

Haeussinger, F. ve Krang, J. (2017). Antecendents of employees information security awareness review, synthesis and directions for future research. . In Proceedings of the 25th European Conference on Information Systems, 5-10 June 2017, Guimarães, Portugal, s. 1-20.

Hair, J. F., Risher, J. J., Sarstedt, M. ve Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2-24.

Haslem, B., Hutton, I. ve Smith, A., H. (2017). How much do corporate defendants really lose? A new verdict on the reputation loss induced by corporate litigation. *Financial Management*, 46(2), 323-358.

Hauk, N., Göritz, A. S. ve Krumm, S. (2019). The mediating role of coping behavior on the age-technostress relationship: A longitudinal multilevel mediation model. *Plos One*, 14(3), 1-22.

Hu, Q., Dinev, T., Hart, P. ve Cooke, D. (2012). Managing employee compliance withinformation security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615-660.

Islam, N., Mavengere, N., Ahlfors, U. R., Ruohonen, M., Serenko, A. ve Palvia, P. (2018). A stressstrain-outcome model of job satisfaction: the moderating role of professional self-efficacy, Twenty-fourth Americas Conference on Information Systems, 16-18 August 2008, New Orleans, LA, s. 1-10.

İlseven, S. (2019). Tekno-stresin çalışanların işten ayrılma niyeti üzerine etkisi. Yüksek lisans tezi, Yükseköğretim Kurulu Ulusal Tez Merkezi, (587252).

Jackson, S. E. ve Schuler, R. S. (1985). A meta-analysis and conceptual critique of research on role ambiguity and role conflict in work settings. *Organizational Behavior and Human Decision Processes, 36*(1), 16-78.

Jeong, C. Y., Lee, S. Y. T. ve Lim, J. H. (2018). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, 56(5), 681-695.

Johnson, M. E. ve Goetz, E. (2007). Embedding information security into the organization. *IEEE Security and Privacy Magazine*, 5(3), 16-24.

Johnston, A. C. ve Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566.

Karasek, R. A. (1979). Job demands, job decision latitude, and mental strain: Implications for job redesign. *Administrative Science Quarterly*, 24(2), 285-308.

Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., Pestell, G., Button, M. ve Wang, V. (2017). Cyber security breaches survey 2017. 20 Eylül 2022 tarihinde https://www.researchgate.net/publication/316432227_Cyber_security_breaches_survey_2017_main_report/references adresinden erişildi.

Kline, R. B. (2016). *Principles and Practice of Structural Equation Modeling*. Fourth edition. New York: The Guilford Press.

Kopuz, E. (2013). Hemşirelerde işe bağlı gerginlik düzeyinin belirlenmesi ve stresle baş etme tutumlarının incelenmesi: Özel bir hastane örneği. Yüksek lisans tezi, Yükseköğretim Kurulu Ulusal Tez Merkezi, (340672).

Kopuz, K. ve Aydın, G. (2020). Sağlık çalışanlarında teknostres: Bir özel hastane örneği. *Ekonomi İşletme ve Maliye Araştırmaları Dergisi*, 2(3), 249-264. https://doi.org/10.38009/ekimad.780928

Lazarus, R. S. (1984). On the primacy of cognition. *American Psychologist, 39*(2), 124-129.

Lazarus, R. S. ve Folkman, S. (1984). *Stress, Appraisal and Coping*. New York, NY: Springer Publishing Company.

Leach, J. (2003). Improving user security behavior. *Computer & Science,* 22(8), 685-692.

Lee, A. R., Son, S. M. ve Kim, K. K. (2016). Information and communication technology overload and social networking service fatigue: A stress perspective. *Computers in Human Behavior, 55,* 51-61.

Lee, R. T. ve Ashforth, B. E. (1996). A meta-analytic examination of the correlates of the three dimensions of job burnout. *Journal of Applied Psychology, 81*(2), 123-133.

Lehto, M. R. ve Landry, S. J. (2012). *Introduction to Human Factors and Ergonomics for Engineers*. New York: CRC Press.

Lewis, J. (2003). Cyber terror: Missing in action. *Knowledge, Technology & Policy*, 16(2), 34-41.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. ve Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13–24.

Liu, Y. ve Keller, R. T. (2021). How psychological safety impacts R&D project teams' performance: In a psychologically safe workplace, R&D project teams perform better, more readily share knowledge and engage in organizational citizenship behavior, and are less likely to leave. *Research-Technology Management*, 64(2), 39-45.

Malhotra, N. K. (2004). *Marketing Research an Applied Orientation*. New Jersey: Pearson Prentice Hall.

Merdan, E. (2021). Teknostresin ve iş geriliminin hizmet inovasyon davranışı üzerine etkisinde esnek çalışma düzenlemelerinin aracılık rolü: Çağrı merkezi örneği. Doktora tezi, Yükseköğretim Kurulu Ulusal Tez Merkezi, (677811).

Moore, J. E. (2000). One road to turnover: An examination of work exhaustion in technology professionals. *MIS Quarterly*, 24(1), 141-168.

Nisafani, A. S., Kiely, G. ve Mahony, C. (2020). Workers' technostress: A review of its causes, strains, inhibitors, and impacts. *Journal of Decision Systems*, 29(1), 243-258.

Özer, A. (2011). Bilginin yolculuğunda bilgi çalışanlarının rolü. *Çimento Endüstrisi İşverenleri Sendikası Dergisi*, 63, 4-20.

Öztemiz, S. ve Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği, *Bilgi Dünyası Dergisi*, 14(1), 87-100. https://doi.org/10.15612/BD.2013.136

Park, H. ve Cho, J. (2016). The influence of ınformation security technostress on the job satisfaction of employees, *Journal of Business and Retail Management Research*, 11(1), 66-75.

Peterson, S. A. (1999). School district central office power and student performance. *School Psychology International*, 20(4), 376-387.

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

Piko, B. (1999). Work-related stress among nurses: a challenge for health care institutions. *The Journal of the Royal Society for the Promotion of Health*, 119(3), 156-162.

Pirkkalainen, H., Salo, M., Tarafdar, M. ve Makkonen, M. (2019). Deliberate or instinctive? Proactive and reactive coping for technostress. *Journal of Management Information Systems,* 36(4), 1179-1212.

Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S. ve Tu, Q. (2008). The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information Systems Research,* 19(4), 417-433.

Ransbotham, S. ve Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, 20(1), 121-39.

Rodoplu, D. (2008). Bilgi teknolojileri uygulamalarına karşı çalışan direnci: Hastane bilgi sistemi üzerinde bir uygulama. *Review of Social, Economic & Business Studies*, 9(10), 409-437.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93-114.

Romanosky, S. (2016). Examing the costs and causes of cyber incidents, *Journal of Cybersecurity*, 2(2), 121-135.

Sabuncuoğlu, Z. ve Tüz, M. (2003). *Örgütsel Psikoloji*, Bursa, Türkiye: Furkan Ofset.

Saganuwan, M. U., Ismail, W. K. W. ve Ahmad, U. N. U. (2015). Conceptual framework: AIS Technostress and its effect on professionals' job outcomes. *Asian Social Science*, 11(5), 97-107.

Salanova, M., Llorens, S., Cifre, E. ve Nogareda, C. (2007). Technostress: Concept, measurement, and prevention. *Notatechia de Prevencion, 730*.

Salanova, M., Rodríguez-Sánchez, A. M., Schaufeli, W. B. ve Cifre, E. (2014). Flowing together: A longitudinal study of collective efficacy and collective flow among workgroups. *The Journal of Psychology*, 148(4), 435-455.

Salmela, H. (2008). Analysing business losses caused by information systems risk: a business process analysis approach. *Journal of Information Technology*, 23(3), 185-202.

Salo, M., Pirkkalainen, H., Makkonen, M. ve Hekkala, R. (2018). Distress, eustress, or no stress? Explaining smartphone users' different technostress responses, Thirty Ninth International Conference on Information Systems, 13-16 December 2018, San Francisco, ss. 1-17.

Sareen, P. (2019). Techno stress creators -An exploratory research on teaching and non teaching staff working in colleges. *International Journal of Management and Humanities*, 3(9), 1-7.

Shadbad, F. N. ve Biros, D. (2020). Technostress and its influence on employee information security policy compliance. *Information Technology and People*, 35(1), 119-141.

Siponen, M. ve Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-502.

Srivastava, S. C., Chandra, S. ve Shirish, A. (2015). Technostress creators and job outcomes: Theorising the moderating influence of personality traits. *Information Systems Journal*, *25*(4), 355-401.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276.

Straub, D. ve Karahanna, E. (1998). Knowledge worker communications and recipient availability: Toward a task closure explanation of media choice. *Organization Science*, 9(2), 160-75.

Sudareswaran, V. (2018). Study of cybersecurity in data breaching. *International Journal of Advancing Engineering and Research Development*, 5(3), 1513-1516.

Şimşek-Demirbağ, K. ve Yıldırım, N. (2021). Can technology substitute its creator? Impact of industry 4.0 on engineering work. *European Proceedings of Social and Behavioural Sciences*, 101, 142-151.

Tarabah, N. E. (2021). The impact of technostress and covid-19 stress on employee burnout among employees in Turkey under the mediating role of resilience. Yüksek lisans tezi, Yükseköğretim Kurulu Ulusal Tez Merkezi, (695298).

Tarafdar, M., Cooper, C. L. ve Stich, J. F. (2019). The technostress trifecta techno eustress, techno distress and design: Theoretical directions and an agenda for research, *Information Systems Journal*, 29(1), 6-42.

Tarafdar, M., D'Arcy, J., Turel, O. ve Gupta, A. (2015). The dark side of information technology. *MIT Sloan Management Review*, 56(2), 61-70.

Tarafdar, M., Ragu-Nathan, T. S., Ragu-Nathan, B. ve To, Q. (2007). The impact of technostress on productivity. *Journal of Management Information Systems Summer*, 24(1), 301-328.

Tarafdar, M., Tu, Q. ve Ragu-Nathan, T. S. (2010). Impact of technostress on end-user satisfaction and performance. *Journal of Management Information Systems*, 27(3), 303-34.

Tarafdar, M., Tu, Q. ve Ragu-Nathan, T. S. (2011). Crossing to the dark side: Examining creators, outcomes and inhibitors of technostress. *Connunications of The Acm*, 54(9), 111-120.

Tekerek, M. (2008). Bilgi güvenliği yönetimi. *Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Dergisi*, 11(1), 132-137.

Torres, C. C. (2021). Adaptation and validation of technostress creators and technostress inhibitors inventories in a Spanish-Speaking Latin American Country. *Technology in Society*, 66, 1-14.

Trevino, L. K. (1992). Experimental approaches to studying ethical-unethical behavior in organizations. *Business Ethics Quarterly*, 2(2), 121-36

Turel, O. ve Gaudioso. F. (2018). Techno-stressors, distress and strain: The roles of leadership and competitiven climates. *Cognition, Technology & Work*, 20(2), 309-24.

Türen, U., Erdem, H. ve Kalkın, G. (2015). İşyerinde tekno-stres ölçeği: Havacılık ve bankacılık sektöründe bir araştırma. *Çalışma İlişkileri Dergisi,* 6(1), 1-19.

URL-1, https://www.bitdefender.com/blog/hotforsecurity/top-5-corporate-losses-due-to-hacking/ 17 Mayıs 2012.

URL-2, https//:www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet 26 Ekim 2016.

Vural, Y. ve Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme, *Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi*, 23(2), 507-522.

Walinga, J. ve Stangor, C. (2014). *Introduction to Psychology*. J. Walinga (Der.). Stress, health, and coping içinde (ss. 742-772). BCcampus.

Wall, J. ve Iyer, L. (2012). The dark side of leadership in information systems security: A model of the effect of manager transgressions on employee security behaviors. Proceedings of the 18th Americas Conference on Information Systems, 9-12 August, 2012, Seattle, WA, s. 1-10.

Wang, K., Shu, Q. ve Tu, Q. (2008). Technostress under different organizational environments: An empirical investigation. *Computers in Human Behavior*, 24, 3002-3013.

Wang, Y., Zheng, Y. ve Zhu, Y. (2018). How transformational leadership influences employee voice behavior: The roles of psychological capital and organizational identification. *Social Behavior and Personality: An International Journal*, 46(2), 313-321.

Weil, M. M. ve Rosen, L. D. (1997). *TechnoStress: Coping with Technology @Work @Home @Play*. California: John Wiley.

Widup, S. (2018, 11 Nisan). 2018 Data breach investigations report. 4 Ekim 2022 tarihinde https://www.researchgate.net/publication/32445535 adresinden erişildi.

Williams, J. ve MacKinnon, D. P. (2008). Resampling and distribution of the product methods for testing indirect effects in complex models. *Structural Equation Modeling: A Multidisciplinary Journal*, 15(1), 23-51.

Willison, R. ve Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1-20.

Yener, S. (2018). Teknostresin iş performansı üzerindeki etkisi: Tükenmişliğin aracı rolü. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi,* 20(2), 85-101. https://doi.org/10.32709/akusosbil.403114

Zainun, N. F., Johari, J. ve Adnan, Z. (2019). Technostress and commitment to change: The moderating role of internal communication. *International Journal of Public Administration*, 43(15), 1327-1339.

Zhao, X., Xia, Q. ve Huang W. (2020). Impact of technostress on productivity from the theoretical perspective of appraisal and coping processes. *Information & Management*, 57(8), 103265.

EKLER

Ek 1. Anket Formu

Teknostresin Bilgi Güvenlik İhlali Etkisinde Tekno Gerilimin Aracı Rolü

Sayın Katılımcı;

Bu çalışma, teknostresin bilgi güvenlik ihlali, üretkenlik ve yıpranmanın etkisi altındayken teknolojik gerilimin aracı rolü üzerine yapılan bilimsel bir araştırma için hazırlanmıştır. Araştırma sonuçlarımızdan sağlıklı sonuçlar elde edebilmemiz, vereceğiniz cevapların gerçek duygu ve düşüncelerinizi yansıtmasına bağlıdır. Çalışma boyunca sizlere yöneltilen maddelerde doğru ya da yanlış cevap söz konusu değildir. İlgili maddeler içerisinde size en yakın olan cevabı işaretlemeniz beklenmektedir. Araştırmada gönüllülük esastır ve vereceğiniz cevaplar araştırma amacı dışında hiçbir yerde kullanılmayacaktır.

Çalışmaya zaman ayırdığınız ve katkı sağladığınız için teşekkür ederiz.

ANKET SORULARI

Demografik Özellikler

Yapılan bu bilimsel çalışmaya gönüllü olarak katılmayı kabul ediyorum.

( ) Evet ( ) Hayır

Cinsiyetiniz?

( ) Kadın ( ) Erkek

Yaşınız?.....

Mesleğiniz?.....

Çalıştığınız sektör?

( ) Bilişim Teknolojileri ( ) Eğitim ( ) Elektrik ve Elektronik ( ) Enerji ( ) Finans ( ) İş ve Yönetim ( ) Medya, İletişim ve Yayıncılık ( ) Metal ( ) Sağlık ve Sosyal Hizmetler ( ) Spor ve Rekreasyon ( ) Ticaret (Satış ve Pazarlama) ( ) Toplumsal ve Kişisel Hizmetler ( ) Ulaştırma, Lojistik ve Haberleşme ( ) Diğer Sektörler

Sektördeki deneyim yılınız nedir?.....

Eğitim Durumunuz?

( ) İlkokul-Orta Okul ( ) Lise Mezunu ( ) Ön Lisans ( ) Lisans ( ) Yüksek Lisans

Çalıştığınız kurumun bilgi güvenliği ihlalinin önüne geçmek adına bir politikası var mıdır?

( ) Evet ( ) Hayır

İş yeri dışında herhangi bir yerde mesai yapıyor musunuz? (Ev, kafe...vs.)

( ) Evet ( ) Hayır

Çalıştığınız kurum bilgi güvenliği ihlali hakkında oryantasyon eğitimi verir mi?

( ) Evet ( ) Hayır

Şirketinizdeki çalışan sayısı kaçtır?

( ) 0-50 ( ) 51-100 ( ) 101-500 ( ) 501-1000 ( ) 1000 ve üzeri

Teknostres ölçeği

Aşağıdaki soruları inceleyerek katılım derecenizi gösteren seçeneği işaretleyiniz.**1-Kesinlikle katılmıyorum 2-Katılmıyorum 3-Kararsızım 4-Katılıyorum 5-Kesinlikle Katılıyorum**		**Kesinlikle Katılmıyorum**	**Katılmıyorum**	**Kararsızım**	**Katılıyorum**	**Kesinlikle Katılıyorum**
1	Bu teknoloji nedeniyle daha hızlı çalışmak zorunda kaldım.	1	2	3	4	5
2	Bu teknoloji nedeniyle üstesinden gelebileceğimden çok daha fazla çalışmak zorunda kaldım.	1	2	3	4	5
3	Bu teknoloji nedeniyle çok sıkı bir iş programı ile çalışmak zorunda kaldım.	1	2	3	4	5
4	Yeni teknolojilere uyum sağlayabilmek için iş alışkanlıklarımı değiştirmek zorunda kaldım.	1	2	3	4	5
5	Teknolojinin karmaşıklığının artması yüzünden iş yüküm arttı.	1	2	3	4	5
6	Bu teknoloji yüzünden ailemle daha az zaman geçiriyorum..	1	2	3	4	5
7	Bu teknoloji yüzünden tatildeyken bile işimle temas halinde olmak zorundayım	1	2	3	4	5
8	Yeni teknolojilere ayak uydurmak için tatil ve hafta sonlarından fedakarlık etmek zorundayım.	1	2	3	4	5
9	Kişisel hayatımın bu teknolojiler tarafından işgal edildiğini hissediyorum.	1	2	3	4	5
10	İşimi tatmin edici bir şekilde yapabilecek kadar bu teknolojiyi bilmiyorum.	1	2	3	4	5
11	Yeni teknolojileri anlamak ve kullanmak için uzun bir zamana ihtiyaç duyarım.	1	2	3	4	5
12	Teknoloji becerilerimi geliştirmek ve öğrenmek için yeterli zaman bulamıyorum.	1	2	3	4	5
13	İş yerinde yeni çalışmaya başlayanların bilgisayar teknolojisi hakkındaki bilgilerinin benimkinden daha fazla olduğunu düşünürüm.	1	2	3	4	5
14	Yeni teknolojileri anlama ve kullanmanın genellikle benim için fazla karmaşık olduğunu düşünürüm.	1	2	3	4	5
15	Yeni teknolojiler yüzünden sürekli iş güvencemi kaybetme tehdidi yaşıyorum.	1	2	3	4	5
16	Yerimi kaybetmemek için teknoloji becerilerimi sürekli geliştirmek zorundayım.	1	2	3	4	5
17	Daha yeni teknoloji becerileri olan iş arkadaşlarımın tehdidine maruz kalmaktayım.	1	2	3	4	5

18	Yerimi alacaklarından korktuğum için iş arkadaşlarımla bilgimi paylaşmam..	1	2	3	4	5
19	Yerlerini kaybetme korkusu nedeniyle iş arkadaşları arasında bilgi paylaşımının daha az olduğunu düşünürüm.	1	2	3	4	5
20	İş yerinde kullandığımız teknolojilerde sürekli yeni gelişmeler vardır.	1	2	3	4	5
21	İş yerindeki bilgisayar yazılımlarında sürekli değişim vardır.	1	2	3	4	5
22	İş yerindeki bilgisayar donanımında sürekli değişim vardır.	1	2	3	4	5
23	İş yerindeki bilgisayar ağlarında sık sık geliştirmeler(güncellemeler) vardır.	1	2	3	4	5

Gerginlik ölçeği

Aşağıdaki soruları inceleyerek katılım derecenizi gösteren seçeneği işaretleyiniz.**1-Kesinlikle katılmıyorum 2-Katılmıyorum 3-Kararsızım 4-Katılıyorum 5-Kesinlikle Katılıyorum**		**Kesinlikle Katılmıyorum**	**Katılmıyorum**	**Kararsızım**	**Katılıyorum**	**Kesinlikle Katılıyorum**
1	Teknoloji kullanmamı gerektiren faaliyetlerden dolayı tükenmiş hissediyorum.	1	2	3	4	5
2	Teknolojiyle ilgili faaliyetlerimden yorgun hissediyorum.	1	2	3	4	5
3	Tüm gün farklı teknolojilerle çalışmak benim için zorlayıcıdır.	1	2	3	4	5
4	Teknolojiyle ilgili faaliyetlerimden tükenmiş hissediyorum.	1	2	3	4	5

Bilgi Güvenliği İhlali Ölçeği

Aşağıda verilen senaryoları okuyarak ilgili sorulardan sizin için en uygun olan seçeneği işaretleyiniz.

SENARYO-1: Parola Paylaşımı

Adem, şirketinizin bir çalışanıdır. Bir gün Adem ofis dışındayken iş arkadaşı Adem'in bilgisayarındaki bir dosyaya ihtiyaç duymuştur. İş arkadaşı, Adem'in yaptığı işe benzer bir iş yapmaktadır. İş arkadaşı Adem'i arar ve ofisteki bilgisayarının parola bilgilerini ister. Adem, ofisteki bilgisayarının parolasını paylaşmaması gerektiğini bilse de şifresini iş arkadaşıyla paylaşır.

1- Bu durumda Adem'le aynı şeyi yapman ne kadar olasıdır?

Çok düşük 1( ) 2( ) 3( ) 4( ) 5( ) Çok olası

2- Adem'in yaptığı gibi böyle bir durumda şifreyi paylaşabilirim.

Kesinlikle katılmıyorum 1( ) 2( ) 3( ) 4( ) 5( ) Kesinlikle katılıyorum

3- Senaryo ne kadar gerçekçidir?

Son derece gerçekçi değil1( ) 2( ) 3( ) 4( ) 5( ) Son derece gerçekçi

SENARYO-2: Aşağıya Parola Yazma

Janset, şirketinizin bir çalışanıdır. Şirket yakın zamanda çalışanların kişisel bilgilerini yönetmek için bir bilgisayar sistemi kurmuştur (Örneğin acil durum çalışan iletişim bilgileri, emeklilik ödenekleri, maaş bilgileri). Her çalışana sistem için bir kullanıcı adı ve şifresi verilmiştir. Janset, kullanıcıların parolalarını kendilerine saklamaları ve başkalarının bilmesine veya kullanmasına izin vermemesi gerektiğini belirten şirket politikasının farkındadır. Ancak, parolasını hatırlamakta zorlanan Janset, bunu yapışkan bir not üzerine yazarak genellikle kullandığı bilgisayar üzerine yapıştırmıştır.

1- Bu durumda Janset'le aynı şeyi yapman ne kadar olasıdır?

Çok düşük 1( ) 2( ) 3( ) 4( ) 5( ) Çok olası

2- Janset'in yaptığı gibi böyle bir durumda şifreyi paylaşabilirim.

Kesinlikle katılmıyorum 1( ) 2( ) 3( ) 4( ) 5( ) Kesinlikle katılıyorum

3- Senaryo ne kadar gerçekçidir?

Son derece gerçekçi değil1( ) 2( ) 3( ) 4( ) 5( ) Son derece gerçekçi

SENARYO-3: Oturumu Kapatmama

Burak, şirketinizin bir çalışanıdır. İşinin bir parçası olarak, Burak'a şirketin bordro sistemine yetkili erişim izni verilmiştir. Burak, iş yerinde bir gün, yönetim için hazırladığı haftalık rapor için bilgi toplamak üzere bordro sistemine giriş yapmıştır. Bir süre sonra Burak tuvalet molasına ihtiyaç duymuştur. Burak kullanıcıların, kullanılmadıklarında bilgisayarlarından çıkış yapmalarını gerektiren şirketin politikasının farkındadır. Ancak Burak, oturumu kapatıp tekrar oturum açmanın verdiği rahatsızlıktan nefret etmektedir. Bu yüzden tuvalete gitmek için masasından ayrıldığında bilgisayarını açık bırakmıştır.

1- Bu durumda Burak'le aynı şeyi yapman ne kadar olasıdır?

Çok düşük 1( ) 2( ) 3( ) 4( ) 5( ) Çok olası

2- Burak'ın yaptığı gibi böyle bir durumda şifreyi paylaşabilirim.

Kesinlikle katılmıyorum 1( ) 2( ) 3( ) 4( ) 5( ) Kesinlikle katılıyorum

3- Senaryo ne kadar gerçekçidir?

Son derece gerçekçi değil1( ) 2( ) 3( ) 4( ) 5( ) Son derece gerçekçi

SENARYO-4: USB Kopyası

Yasemin, şirketinizde bir çalışandır ve şu anda hassas şirket verilerinin analizini gerektiren bir rapor üzerinde çalışmaktadır. Son derece meşguldür ve o akşam ilerleyen saatlerde evde rapor üzerinde çalışmaya devam etmek istemektedir. Yasemin, güvenlik sorunlarını önlemek için kullanıcıların şirket verilerini USB sürücüler gibi taşınabilir medyalara kopyalamasını yasaklayan şirketinizin politikasının farkındadır. Ancak, Yasemin birkaç şirket dosyasını kişisel, şifrelenmemiş bir USB sürücüsüne kopyalar, böylelikle evde rapor üzerinde çalışabilir.

1- Bu durumda Yasemin'le aynı şeyi yapman ne kadar olasıdır?

Çok düşük 1( ) 2( ) 3( ) 4( ) 5( ) Çok olası

2- Yasemin'in yaptığı gibi böyle bir durumda şifreyi paylaşabilirim.

Kesinlikle katılmıyorum 1( ) 2( ) 3( ) 4( ) 5( ) Kesinlikle katılıyorum

3- Senaryo ne kadar gerçekçidir?

Son derece gerçekçi değil1( ) 2( ) 3( ) 4( ) 5( ) Son derece gerçekçi

SENARYO-5: Veri Sızıntısı

Orkun, şirketinizdeki insan kaynakları departmanında görev yapan bir çalışandır ve bu nedenle, tüm çalışanların maaş bilgilerini görüntüleme yetkisine sahiptir. Kısa süre önce, Orkun'un şirkette çalışmayan arkadaşlarından biri Orkun ile iletişime geçmiştir ve şirketinizdeki tüm yöneticilerin maaş bilgilerini istemiştir. Arkadaşı Orkun'a şirketinize bir yönetim pozisyonu için başvurduğunu ve bu pozisyonun kendisine teklif edilmesi durumunda hangi maaşı isteyeceğini belirlemek için bu bilgiye sahip olmak istemiştir. Orkun, maaş bilgilerini sağlamanın şirket politikasının ihlali olduğunu bilse de, bu bilgiyi araştırıp arkadaşını bilgilendirmiştir.

1- Bu durumda Orkun'la aynı şeyi yapman ne kadar olasıdır?

Çok düşük 1( ) 2( ) 3( ) 4( ) 5( ) Çok olası

2- Orkun'un yaptığı gibi böyle bir durumda şifreyi paylaşabilirim.

Kesinlikle katılmıyorum 1( ) 2( ) 3( ) 4( ) 5( ) Kesinlikle katılıyorum

3- Senaryo ne kadar gerçekçidir?

Son derece gerçekçi değil1( ) 2( ) 3( ) 4( ) 5( ) Son derece gerçekçi

SENARYO-6: Bağlantılara Tıklayın

Kübra, şirketinizin bir çalışanıdır ve her gün bazı formları doldurması için bağlantıların bulunduğu birçok e-posta alıyor. Bir gün bilinmeyen bir gönderenden bir e-posta alır. E-postanın kaynağını doğrulamadan bağlantılara tıklamak şirket politikasına aykırı olsa da, e-postanın güvenilir bir kaynaktan gönderildiğini varsayarak bağlantıya tıklar.

1- Bu durumda Kübra ile aynı şeyi yapman ne kadar olasıdır?

Çok düşük 1( ) 2( ) 3( ) 4( ) 5( ) Çok olası

2- Kübra'nın yaptığı gibi böyle bir durumda şifreyi paylaşabilirim.

Kesinlikle katılmıyorum 1( ) 2( ) 3( ) 4( ) 5( ) Kesinlikle katılıyorum

3- Senaryo ne kadar gerçekçidir?

Son derece gerçekçi değil1( ) 2( ) 3( ) 4( ) 5( ) Son derece gerçekçi

ETİK KURUL KARARI

T.C.

GÜMÜŞHANE ÜNİVERSİTESİ REKTÖRLÜĞÜ

BİLİMSEL ARAŞTIRMA VE YAYIN ETİĞİ KURULU

Sayı: E-95674917-108.99-17485

Konu: Etik Kurul Onay

TOPLANTI TUTANAĞI

TARİH :

14/04/2021

SAYI :

2021/3

GÜNDEM:

1. Doç. Dr. Orkun DEMİRBAĞ'ın **"TEKNOSTRESİN BİLGİ GÜVENLİK İHLALİ ETKİSİNDE TEKNO GERİLİMİN ARACI ROLÜ"** konulu başvurusunun görüşülmesi.

KARAR :

1. Doç. Dr. Orkun DEMİRBAĞ' ın dosyası usul ve esas açısından incelendi ve dosyada usul ve esas bakımından bir eksiklik olmadığı belirtilmesi üzerine, dosya kurul üyeleri tarafından projenin yürürlükteki mevzuata uygun olduğuna oy birliği ile karar verildi.

ÖZGEÇMİŞ

Halil İbrahim KAYMAK, Orta öğrenimini Gümüşhane'de ve Lise öğrenimini Trabzon'da tamamladı. 2009 yılında başladığı Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümünü 2013 yılında, 2017 yılında başladığı Anadolu Üniversitesi Havacılık Yönetimi Proğramını 2021 yılında bitirdi, 2019 yılında Gümüşhane Üniversitesi İşletme Anabilim Dalında Yüksek Lisans eğitimine başladı ve halen Gümüşhane Üniversitesi Meslek Yüksekokulunda Öğretim görevlisi olarak görev yapmaktadır.